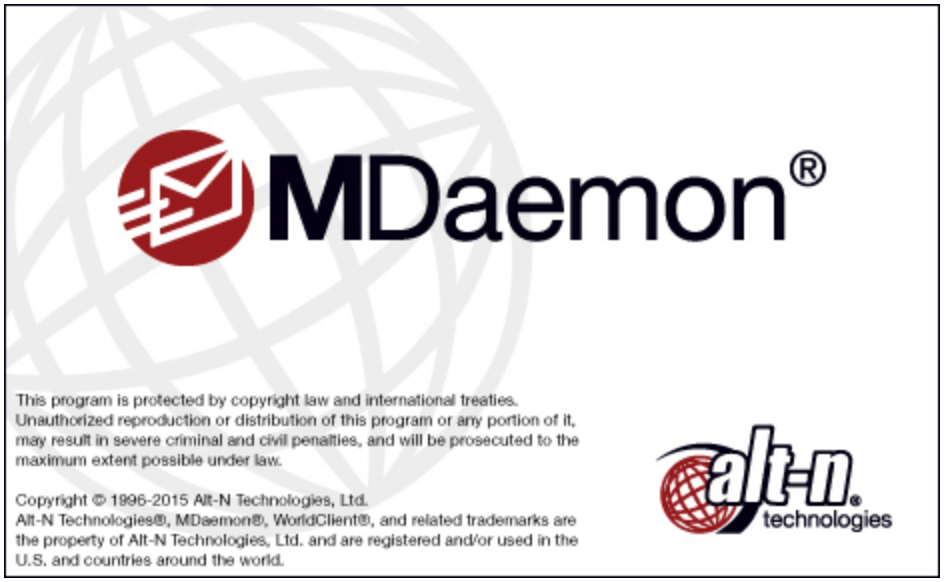

MDaemon®
This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program or any portion of it, may result in severe criminal and civil penalties, and will be prosecuted to the maximum extent possible under law.
Copyright © 1996-2015 Alt-N Technologies, Ltd.
Alt-N Technologies®, MDaemon®, WorldClient®, and related trademarks are the property of Alt-N Technologies, Ltd. and are registered and/or used in the U.S. and countries around the world.
alt-n technologies

User Manual

15.5

MDaemon Messaging Server
User Manual

Copyright © 1996-2015 Alt-N Technologies, Ltd. Alt-N®, MDaemon®, and RelayFax® are trademarks of Alt-N Technologies, Ltd.

BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™, BBM™ and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world. Used under license. Apple is a trademark of Apple Inc. Windows Mobile, Microsoft and Outlook are trademarks of Microsoft Corporation. Palm is a trademark of Palm Trademark Holding Company, LLC. All other trademarks are the property of their respective owners.

v15.5.0 - September 2015

Table of Contents

Section I MDaemon Messaging Server 15.5 12

1 MDaemon Features ... 12
2 System Requirements ... 14
3 New in MDaemon 15.5 ... 15
4 Upgrading to MDaemon 15.5.0 ... 31
5 Getting Help ... 35

Section II MDaemon's Main Display 40

1 Stats ... 40
2 Event Tracking and Logging ... 41
Event Tracking Window's Shortcut Menu ... 43
3 Composite Log View ... 44
4 Tray Icon ... 44
Shortcut Menu ... 45
Locking/Unlocking MDaemon's Main Interface ... 46
5 Session Window ... 46
6 MDaemon's SMTP Work Flow ... 47

Section III Setup Menu 50

1 Server Settings ... 50
Server Settings ... 50
Delivery ... 50
Servers ... 53
Ports ... 56
DNS ... 58
IPv6 ... 60
Binding ... 61
Timeouts ... 62
Sessions ... 64
Mail Release ... 66
On-Demand Mail Relay (ODMR) ... 68
Archiving ... 69
Pruning ... 71
Message Recall ... 72
Unknown Mail ... 73
Domain Sharing ... 75
Priority Mail ... 77
IP Cache ... 79
Header Translation ... 81
Header Translation Exceptions ... 82
Default Signatures ... 83
Public & Shared Folders ... 84
Public & Shared Folders ... 87
DomainPOP ... 88

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Host & Settings ... 90
Parsing ... 93
Processing ... 95
Routing ... 96
Foreign Mail ... 98
Name Matching ... 99
Archive ... 100
RAS Dialup Settings ... 101
RAS ... 101
Logon ... 103
Processing ... 104
LDAP/Address Book Settings ... 105
LDAP ... 106
Logging ... 109
Log Mode ... 109
Composite Log ... 111
Statistics Log ... 112
Windows Event Log ... 114
Maintenance ... 115
Settings ... 116
2 Domain Manager ... 121
Host Name & IP ... 124
Smart Host ... 125
Accounts ... 128
WCIM ... 130
Calendar ... 132
WorldClient Settings ... 134
Signatures ... 138
Settings ... 140
ActiveSync for MDaemon ... 142
Client Settings ... 143
Policy Manager ... 146
Assigned Policy ... 155
Clients ... 156
3 Gateway Manager ... 162
Global Gateway Settings ... 165
Automatic Gateway Creation ... 166
Gateway Editor ... 168
Domain ... 168
Verification ... 170
Configuring Multiple LDAP Verification Queries ... 172
Forwarding ... 174
Dequeuing ... 175
Quotas ... 177
Settings ... 179
4 Mailing List Manager ... 180
Mailing List Settings ... 183
Mailing List Editor ... 186
Members ... 186
Settings ... 189
Enhanced List Pruning ... 191
Headers ... 192
Subscription ... 194

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Subscribing to Mailing Lists ... 196
Reminders ... 198
Digest ... 199
Notifications ... 201
Moderation ... 202
Routing ... 204
Support Files ... 206
Public Folder ... 208
Active Directory ... 209
ODBC ... 211
Configuring an ODBC Data Source ... 212
Creating a New ODBC Data Source ... 214
5 Public Folder Manager ... 218
Access Control List ... 220
6 Web & IM Services ... 224
WorldClient (web mail) ... 224
Overview ... 224
Calendar & Scheduling System ... 225
WorldClient Instant Messenger ... 225
Instant Messaging ... 226
Automatic Address Book Synchronization ... 227
Using WorldClient ... 228
Web Server ... 229
Running WorldClient under IIS6 ... 231
SSL & HTTPS ... 234
Dynamic Screen ... 237
WCIM ... 239
Calendar ... 241
Free/Busy Options ... 241
CalDAV ... 243
RelayFax ... 246
Settings ... 247
Branding ... 250
Remote Administration ... 251
Web Server ... 252
SSL & HTTPS ... 255
Running Remote Administration under IIS ... 258
Attachment Linking ... 262
7 Event Scheduling ... 265
AntiVirus Scheduling ... 265
AntiVirus Updates ... 265
Schedule ... 267
Mail Scheduling ... 269
Mail Sending & Collecting ... 269
MultiPOP Collection ... 272
Mail Schedule ... 273
8 Mobile Device Management ... 276
ActiveSync for MDaemon ... 276
ActiveSync for MDaemon ... 276
Protocol Restrictions ... 278
Client Settings ... 280
Policy Manager ... 284
Domains ... 292

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Clients ... 297
Accounts ... 303
Security ... 308
Diagnostics ... 310
Tuning ... 312
BlackBerry Enterprise Server ... 314
Status ... 318
Policies ... 319
Domains ... 326
MDS-CS ... 327
Devices ... 328
Backup/Restore ... 329
Settings ... 330
BlackBerry Internet Service ... 335
Domains ... 336
Subscribers ... 338
Settings ... 340
SyncML ... 342
Configuring Your SyncML Clients ... 343
9 Preferences ... 344
Preferences ... 344
UI ... 344
System ... 347
Disk ... 349
Fixes ... 351
Headers ... 352
Miscellaneous ... 354
Windows Service ... 356
Section IV Security Menu 360
1 Content Filter and AntiVirus ... 362
Content Filter Editor ... 364
Rules ... 364
Creating a New Content Filter Rule ... 366
Modifying an Existing Content Filter Rule ... 370
Using Regular Expressions in Your Filter Rules ... 370
Attachments ... 375
Notifications ... 376
Message Macros ... 377
Recipients ... 380
Compression ... 381
AntiVirus ... 383
AntiVirus ... 383
AV Updater ... 386
Updater Configuration Dialog ... 388
2 Outbreak Protection ... 389
3 MDPGP ... 394
4 Spam Filter ... 401
Spam Filter ... 401
Spam Filter ... 402
Bayesian Classification ... 405
Bayesian Auto-learning ... 409

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Spam Daemon (MDSpamD) ... 411
White List (automatic) ... 413
White List (no filtering) ... 416
White List (by recipient) ... 417
White List (by sender) ... 418
Black List (by sender) ... 419
Updates ... 420
Reporting ... 421
Settings ... 422
DNS Black Lists (DNS-BL) ... 425
Hosts ... 426
White List ... 427
Settings ... 428
Auto-generating a Spam Folder and Filter ... 430
Spam Honeypots ... 431
5 Security Settings ... 432
Security Settings ... 432
Relay Control ... 432
Reverse Lookup ... 434
POP Before SMTP ... 437
Trusted Hosts ... 438
Trusted IPs ... 439
Sender Authentication ... 440
IP Shield ... 440
SMTP Authentication ... 442
SPF Verification ... 444
DomainKeys Identified Mail ... 446
DKIM Verification ... 447
DKIM Signing ... 450
DKIM Settings ... 453
DMARC ... 455
DMARC Verification ... 462
DMARC Reporting ... 464
DMARC Settings ... 468
Message Certification ... 469
VBR Certification ... 471
Approved List ... 474
Screening ... 475
Sender Blacklist ... 475
Recipient Blacklist ... 477
IP Screen ... 478
Host Screen ... 480
Dynamic Screen ... 482
Hijack Detection ... 486
SSL & TLS ... 487
MDaemon ... 489
WorldClient ... 492
Remote Administration ... 495
STARTTLS White List ... 499
STARTTLS Required List ... 500
Creating and Using SSL Certificates ... 500
Creating a Certificate ... 500
Using Certificates Issued by a 3rd party ... 500
Other ... 502

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Backscatter Protection - Overview ... 502
Backscatter Protection ... 504
Bandwidth Throttling - Overview ... 506
Bandwidth Throttling ... 507
Tarpitting ... 508
Greylisting ... 510
LAN Domains ... 513
LAN IPs ... 514
Site Policy ... 515

Section V Accounts Menu 518

1 Account Manager ... 518

Account Editor ... 521
Account Details ... 521
Mail Folder & Groups ... 524
Mail Services ... 525
Web Services ... 526
Autoresponder ... 529
Forwarding ... 533
Restrictions ... 534
Quotas ... 537
Attachments ... 539
IMAP Filters ... 541
MultiPOP ... 544
Aliases ... 546
Shared Folders ... 547
Access Control List ... 548
BlackBerry Enterprise Server ... 553
BlackBerry Internet Service ... 556
ActiveSync for MDaemon ... 557
Client Settings ... 558
Assigned Policy ... 561
Clients ... 562
Signature ... 568
Administrator Notes ... 569
Administrative Roles ... 570
White List ... 571
Settings ... 573

2 Groups & Templates ... 576

Group Manager ... 576
Group Properties ... 577
Template Manager ... 580
Template Properties ... 582
Mail Services ... 585
Web Services ... 587
Autoresponder ... 590
Forwarding ... 594
Quotas ... 596
Attachments ... 599
Administrative Roles ... 601
White List ... 602
Settings ... 604

3 Account Settings ... 605

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Active Directory ... **605**
Monitoring ... 608
Authentication ... 611
Aliases ... **613**
Aliases ... 613
Settings ... 615
Autoresponders ... **617**
Accounts ... 617
White List ... 619
Settings ... 620
Creating Auto Response Scripts ... 621
Auto Response Script Samples ... 624
Outlook Connector for MDaemon ... **625**
Outlook Connector ... 626
Accounts ... 627
Account Database ... **628**
ODBC Selector Wizard ... 629
Creating a New Data Source ... 631
Windows Address Book ... **635**
Passwords ... **636**
Quotas ... **638**
Minger ... **640**
4 Importing Accounts ... **642**
Importing Accounts from a Text File ... **642**
Windows Account Integration ... **644**

Section VI Catalogs Menu 650
1 Catalog Editor ... **650**
2 The PUBLIC Catalog ... **651**

Section VII Queues Menu 654
1 Mail Queues ... **654**
Retry Queue ... **654**
Holding Queue ... **656**
Custom Queues ... **658**
Restore Queues ... **660**
DSN Settings ... **661**
2 Pre/Post Processing ... **663**
3 Queue and Statistics Manager ... **664**
Queue Page ... **665**
User Page ... **668**
Log Page ... **670**
Report Page ... **672**
Customizing the Queue and Statistic Manager ... **673**
MDstats.ini File ... 673
MDStats Command Line Parameters ... 674

Section VIII Additional MDaemon Features 678
1 MDaemon and Text Files ... **678**
2 Remote Server Control via Email ... **678**

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

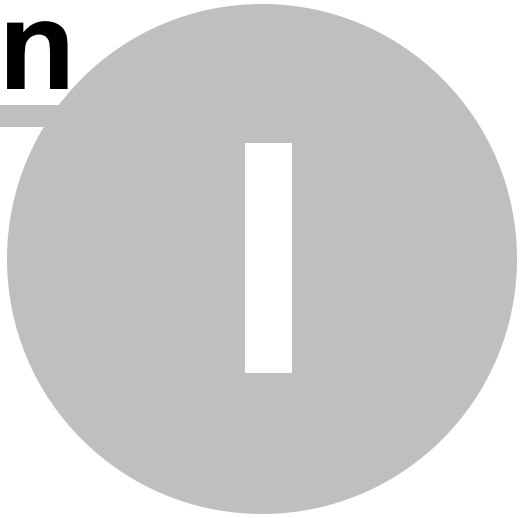
Mailing List and Catalog Control ... 678
General Email Controls ... 681
3 The RAW Message Specification ... 682
The RAW Message Specification ... 682
Bypassing the Content Filter ... 682
RAW Headers ... 682
Special fields supported by RAW ... 683
Sample RAW mail messages ... 684
4 Semaphore Files ... 684
5 Route Slips ... 690
6 MDaemon and Proxy Servers ... 692

Section IX Glossary 694

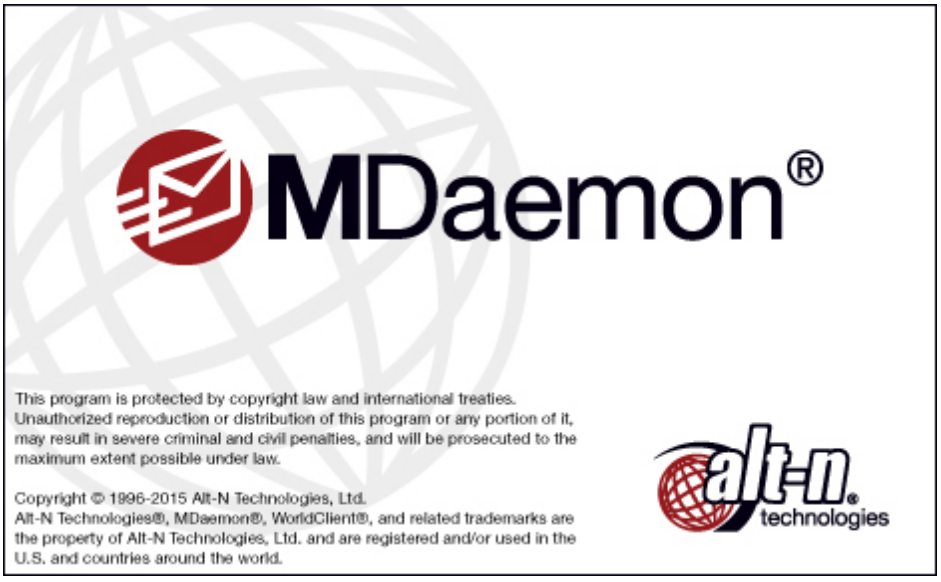
Index 715

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Section



1 MDaemon Messaging Server 15.5


MDaemon®
This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program or any portion of it, may result in severe criminal and civil penalties, and will be prosecuted to the maximum extent possible under law.
Copyright © 1996-2015 Alt-N Technologies, Ltd.
Alt-N Technologies®, MDaemon®, WorldClient®, and related trademarks are the property of Alt-N Technologies, Ltd. and are registered and/or used in the U.S. and countries around the world.
alt-n technologies

Introduction

Alt-N Technologies' MDaemon Messaging Server is a standards-based SMTP/POP3/IMAP mail server that supports Windows 7/Vista/XP/2008/2003 systems and offers a full range of mail server functionality. MDaemon is designed to manage the email needs of any number of individual users and comes complete with a powerful set of integrated tools for managing mail accounts and message formats. MDaemon offers a scalable SMTP, POP3, and IMAP4 mail server complete with LDAP and Active Directory support, an integrated browser-based email client, content filtering, spam filters, extensive security features, and more.

MDaemon Lite and Pro

MDaemon Messaging Server is available in two versions: MDaemon Lite and MDaemon Pro. With the powerful features of MDaemon Lite, you can host your network's email with MDaemon's full-fledged SMTP server, or you can collect your entire domain's email from a single ISP provided POP3 mailbox via the included DomainPOP feature. You can also host multiple Mailing Lists, allow your users to access their email via the included WorldClient webmail component, and utilize a number of other features. MDaemon Pro is equipped with everything in Lite, plus its support for IMAP4, multiple domains, Domain Sharing, Gateways, expanded Mailing Lists, and BlackBerry smartphone integration make it ideal for larger organizations with greater needs. MDaemon Pro also adds group calendar and scheduling, an instant messaging system, multiple language support for WorldClient, automatic domain gateway creation, and more. For a detailed comparison chart outlining the features included in each version, visit: www.altn.com.

MDaemon Features

MDaemon is equipped with many features besides SMTP, POP3, and IMAP4 email processing. The following is a list of just some of those features.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

- MDaemon Pro includes a fully integrated BlackBerry® Enterprise Server, which makes it possible for your users to synchronize their MDaemon email, calendar, contacts, and other PIM data with a BlackBerry device 14.
- Complete support for virus scanning and protection through SecurityPlus for MDaemon. This add-on for MDaemon provides potent anti-virus protection. Messages can be scanned for viruses and cleaned or deleted automatically before ever reaching the intended recipients. Further, you can configure MDaemon to send a message to the administrator, sender, and recipient of the infected message notifying them of the virus. SecurityPlus for MDaemon is a separately licensed product that is available from www.altn.com.
- MDaemon features a complete suite of Mailing List or email group management functions allowing for the formation of an unlimited number of distinct distribution lists that can contain local and/or remote members. Lists can be set to allow or refuse subscription requests, be public or private, post replies to either the list or the originator of the message, be sent in digest format, and be configured using numerous other features.
- An integrated component of MDaemon is WorldClient 224. This exciting product makes it possible for your users to access their email using their favorite web browser rather than from a workstation dependent email client. This tool is perfect for mobile staff and users who do not have a dedicated machine from which to access their email.
- WorldClient is equipped with a complete suite of email client features. You can: send and receive email, spell check messages, manage your email in multiple personal folders, display the interface in any of 18 languages, schedule meetings and appointments and share calendars and tasks with other users, manage your MDaemon account settings (when used in conjunction with Remote Administration 251), manage contacts, and more. WorldClient is also equipped with WorldClient Instant Messenger 225, a small utility that can be downloaded and installed on a user's local computer. This provides easy access to your email and folders and checks for new messages without having to open your web browser. It also includes a complete Instant Messaging system that can be used to quickly "chat" with other MDaemon/WorldClient users.
- MDaemon is equipped with many features designed to help you make your email system secure. The Spam Filter and DNS Black Lists features will help you put an end to most "spam" email messages that "spammers" try to route through or to your domain. IP and Host Screening and the Address Blacklist provide the capability to screen and prevent certain addresses and domains from connecting to or sending mail through your system. They also make it possible to connect to specific IP addresses while screening all others.
- Equipped with support for Lightweight Directory Access Protocol (LDAP), MDaemon can keep your LDAP server up to date on all of its user accounts. This makes it possible for you to keep an LDAP address book up to date so that users with email clients that support LDAP can access it. You can also choose to use Active Directory or your LDAP server as the MDaemon account database instead of an ODBC compliant database or the local `USERLIST.DAT` system. Thus, you can configure multiple MDaemon's at different locations to share the same account database.
- MDaemon's extensive parsing features make it possible to provide email for an

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

entire LAN with as little as a single dial-up ISP POP3 mailbox. This makes it possible to provide email to an entire network for a fraction of the normally associated cost.

- MDaemon can be configured to keep your Windows Address Book or Microsoft Outlook Contact Store up to date with your user information. This provides another means of making a global address book available to your users.
- Address Aliases provides the ability to route email messages addressed to "fictitious" mailboxes to a valid account or mailing list. This makes it possible for individual accounts and lists to have multiple email addresses at one or more domains.
- The Domain Gateways feature provides the option of setting up separate domains for various departments or groups that may be local to your network or located somewhere else on the Internet. Using this feature, all mail addressed to a domain for which MDaemon is acting as a gateway will be placed in that domain's mailbox by MDaemon. It can then be collected by that domain's MDaemon server or email client and distributed to the domain's users. This feature can also be used to enable MDaemon to act as a backup mail server for other domains.
- Accounts can be controlled remotely by users by using specially formatted email messages. This allows greater administrative flexibility, and empowers users by turning day-to-day simple account maintenance tasks, such as changing passwords, over to them.
- Integrated web-based remote administration. MDaemon's Remote Administration 251 component is integrated with MDaemon and WorldClient and enables your users to review and edit their account settings via their web-browser. You can designate which settings that your users may edit, and assign access permissions on a per account basis. Remote Administration can also be used by the Administrator (and whomever else you wish to allow) to review or edit any of MDaemon's settings and any other files that you wish to make available to the Remote Administration system for reviewing.
- With File Catalogs, the email administrator can create password protected groups of files which users can have encoded and automatically sent to them through the use of specially formatted email messages.
- An internal message transport system known as RAW mail provides a simple method for placing messages into the mail stream and greatly simplifies custom mail software development. Using RAW, a complete mail system can be devised using a simple text editor and a couple of batch files.
- A highly versatile Content Filtering system makes it possible for you to customize server behavior based on the content of incoming and outgoing email messages. You can insert and delete message headers, add footers to messages, remove attachments, route copies to other users, cause an instant message to be sent to someone, run other programs, and more.

System Requirements

For the most up to date information on MDaemon's system requirements and recommendations, visit the System Requirements page at www.altn.com.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Certain management, security or wireless synchronization features for BlackBerry smartphones may not be available in all markets. Please refer to the features identified in the product release notes or on the MDaemon messaging server website. Certain functionality requires the activation of a BlackBerry smartphone with a compatible data plan. Check with your service provider for availability, costs and restrictions.

BlackBerry Enterprise Server is not available in some countries and regions.

Trademarks

Copyright © 1996-2015 Alt-N Technologies, Ltd. Alt-N®, MDaemon®, and RelayFax® are trademarks of Alt-N Technologies, Ltd.

BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™, BBM™ and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world. Used under license. Apple is a trademark of Apple Inc. Windows Mobile, Microsoft and Outlook are trademarks of Microsoft Corporation. Palm is a trademark of Palm Trademark Holding Company, LLC. All other trademarks are the property of their respective owners.

See:

New in MDaemon 15.5 15
Upgrading to MDaemon 15.5.0 31
MDaemon's Main Display 40
Getting Help 35

1.3 New in MDaemon 15.5

CALDAV (MDaemon PRO only) 243

MDaemon in now equipped with a CalDAV server. CalDAV is an Internet standard for managing and sharing calendars and scheduling information. MDaemon's CalDAV support makes it possible for your accounts to use any client that supports CalDAV to access and manage their personal calendars and tasks. They can also access any public 218 or shared 547 calendars or tasks according to their access rights 220.

MDPGP Provides OpenPGP Support (MDaemon PRO only) 394

OpenPGP is an industry standard protocol for exchanging encrypted data, and there are a variety of OpenPGP plugins for email clients that make it possible for users to send and receive encrypted messages. MDPGP is MDaemon's integrated OpenPGP component that can provide encryption, decryption, and basic key management services for your users without requiring them to use an email client plugin.

MDPGP encrypts and decrypts emails using a public-key/private-key system. To do

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

this, when you wish to use MDPGP to send a private and secure message to someone, MDPGP will encrypt that message using a "key" that you previously obtained from that person (i.e. his "public key") and imported into MDPGP. Conversely, if he wishes to send a private message to you, then he must encrypt the message using your public key, which he obtained from you. Giving the sender your public key is absolutely necessary, because without it he can't send you an OpenPGP encrypted message. Your unique public key must be used to encrypt the message because your unique private key is what MDPGP will use to decrypt the message when it arrives.

In order for MDPGP to manage signing, encrypting, and decrypting messages, it maintains two stores of keys (i.e. keyrings)—one for public keys and one for private keys. MDPGP can generate your users' keys automatically as needed, or you can create them manually for specific users. You can also import keys that were created elsewhere. Further, MDaemon can look for public keys attached to authenticated messages from local users, and then import those keys automatically. That way a user can request a public key from someone and then email that key to himself so that MDPGP will detect it and then import it into the public keyring. Finally, whenever a message arrives for an address that has a key in a keyring, MDPGP will sign, encrypt, or decrypt the message as needed, according to your settings.

You can configure MDPGP's signing and encryption services to operate either automatically or manually. When set to operate automatically, MDPGP will automatically sign and encrypt messages whenever possible. When set to operate manually, MDPGP will only sign or encrypt a message when the sending user inserts a special command into the message's Subject. In any case messages will only be signed or encrypted (or decrypted) when the account has been given permission to use those services.

Do Not Disturb 577

Do Not Disturb is a new Group Properties feature 577 that makes it possible for you to schedule a time frame during which an account may not send mail or be accessed by its users. Access during a Do Not Disturb period is not allowed and returns an appropriate error response to IMAP, POP, SMTP, ActiveSync, and WorldClient access requests. MDaemon will still accept incoming mail for accounts in this state, but those accounts may not send mail or be accessed by mail clients.

ActiveSync Redesigned 276

The ActiveSync for MDaemon interface was completely redesigned, and there are a variety of new features and policy options available. You can manage ActiveSync under Mobile Device Management 276, the Domain Manager 142, and on the Account Editor 557.

UI Improvements

- There is now an Accounts 128 screen on the Domain Manager, to more easily access accounts while managing a domain.
- The Account Manager 518 and Domain Accounts 128 screens now have a right-click menu with common shortcuts, such as: enable, disable, and properties.
- The DNS 58 screen was redesigned.
- Added options to Preferences » UI 344 to center dialogs when opening, to split

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

the Sessions tab in the main MDaemon UI 41 into its own pane, and to display system generated lists (e.g. Everyone@ and MasterEveryone@) in the Mailing List Manager 180.

WorldClient Improvements

- Modernized the LookOut theme's icons and colors, and made some adjustments to its layout. There is also a new gray color style, although the default style is blue. The "New" button was moved to where the user's email address was previously located, and the email address is now in the top navigation bar. The Help and Sign Out options were moved to a drop-down list beneath user's address, like in the WorldClient theme. Finally, the Options icon was moved to the far right in the navigation bar.
- WorldClient now supports adding inline images to a user's signature.
- Merged Categories and Labels into just Categories. Users can now add, edit, and delete categories from a predefined list based on the old labels and categories. Each category has a color associated with it. More than one category can be associated with a given color, but only one category with a specific name may exist. There are 26 colors to choose from (including white) which match Outlook category color options. If an event, task, note, or contact already has categories associated with it, but they don't match the predefined categories, their colors will be white until the user adds them to the predefined list of categories. If there is already a label associated with an event, the user can choose to remove the label and add a category, or leave the label. Old labels are not lost on upgrade.
- WorldClient and LookOut themes - Desktop notifications are now available. When LookOut or WorldClient loads, the browser will prompt the user on whether or not to allow desktop notifications. If the user chooses to allow them, then the user will receive notifications of new email messages, new instant messages (in the case that the corresponding chat is not in focus), and any change in status of a chat buddy. Desktop notifications are not supported by Internet Explorer.
- WorldClient and LookOut themes - Added ability to view pdf files in the browser (not supported in IE8). This is available in any document folder and any message that has a pdf file.
- There is now a Password Recovery feature 247 in WorldClient. When this feature is enabled, users who have permission to edit their password 526 will be able to enter an alternate email address in WorldClient, which can be sent a link to reset their password if they forget it. To set up this feature, users must enter both the password recovery email address and their current password in WorldClient on the Options » Personalize page. Once set, if the user attempts to log in to WorldClient with an incorrect password a "forgot password?" link will appear. This link takes them to a page that asks them to confirm their password recovery email address. If entered correctly, an email will be sent with a link to a change password page.
- LookOut and WorldClient themes - added buttons and context menu items for users to create a new event, task, or note from the contents of a message.
- Lite, LookOut, and WorldClient themes now attempt to detect and use the language currently being used by the browser.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

- LookOut and WorldClient themes - users can now use the browser's back and forward buttons to navigate in the main window
- LookOut and WorldClient themes - Virtru can now be disabled by the admin on a per user basis by adding `VirtruDisabled=Yes` to the `[User]` section of the user's `WC\User.ini` file.
- WorldClient theme - added a "Today" button to the calendar view buttons.
- LookOut and WorldClient themes - users can now sort by the Description, Location, Start, and End columns in the Calendar List view
- Lite, LookOut, and WorldClient themes - Added <ROOT> as top most option when creating or editing a folder.
- LookOut and WorldClient themes - added button to send a message to all attendees of a meeting in the event editor.
- Lite theme - a Mark Unread/Read option is now available in the Message view. Clicking it will mark the message unread and take the user back to the List view.
- Lite, LookOut, and WorldClient themes - users can now print the details of a single event.
- LookOut and WorldClient themes - there is now a "custom intro" feature in the compose window for Virtru encrypted messages

Additional Features and Changes

MDaemon 15.5 has many more new features and changes. See `RelNotes.html` located in MDaemon's `\Docs\` subfolder for a complete list of all new features, changes, and fixes to MDaemon from the previous version.

New in MDaemon 15.0

IPv6 Support (MDaemon PRO only)

MDaemon now supports IPv6 60. MDaemon will detect the level of IPv6 capability that your OS supports and dual-stack where possible; otherwise, MDaemon will monitor both networks independently. Outbound SMTP, POP, and IMAP connections will prefer IPv6 over IPv4 whenever possible.

When MDaemon connects to an IPv6 host it must use an IPv6 local address of its own. Therefore the Domain Manager's Host Name & IP 124 screen now contains a separate edit control where you can specify an IPv6 address for the domain to use. If this IPv6 address is missing MDaemon will try to automatically detect a suitable address for use. Buttons to manually detect and designate IP addresses were also added to the same screen.

Finally, $PRIMARYIP6$ and $DOMAINIP6$ macros can be used to retrieve IPv6 addresses. These macros can be used anywhere that the $PRIMARYIP$ and $DOMAINIP$ macros can be used.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Improved UI

MDaemon 15.0 includes a number of improvements to the user interface:

New Access Control List (ACL) Editor

The ACL editor 220 was completely redesigned. It now includes more information about the item you are editing and has search features for added new users or groups to the ACL.

Mailing List Manager

Mailing lists are now administered from the new Mailing List Manager 180, accessed under the Setup menu. Consequently, the Lists menu was removed from the menu bar and several list editor screens were reorganized and redesigned. Further, several list-related global options that were located on the Preferences dialog and the Mailing List Editor were moved to a new Mailing List Settings 183 screen on the Mailing List Manager.

Gateway Manager

Domain gateways are now administered from the new Gateway Manager 162, accessed under the Setup menu. Consequently, the Gateways menu was removed from the menu bar and several Gateway Editor screens were reorganized and redesigned. Further, the Gateway Editor's Account screen was deprecated and removed.

Other UI Changes

Below is a list of additional changes to the MDaemon 15.0 interface. For an exhaustive list of UI changes, see the 15.0 Release Notes.

- The IP Shield 440 was moved from Security Settings to Sender Authentication.
- Mail Scheduling Options was renamed to Mail Sending & Collecting 269.
- All screens named "Options" throughout the interface were renamed to "Settings".
- There is a new Binding 61 screen located under Server Settings. Several options related to inbound and outbound socket binding were moved there from the Preferences dialog. It also contains separate edit controls for IPv4 and IPv6 addresses.
- The WorldClient-related dynamic screening options were moved to a new Dynamic Screen 237 page under WorldClient (web mail).
- The Account Manager 518 contains new options for displaying only accounts that are forwarding mail, are over-quota, or have autoresponders configured.

Improved Hijack Detection (MDaemon PRO only)

Hijack Detection 486 was expanded, allowing you to define different message and timing thresholds based on whether the connecting IP address is a reserved IP, a local IP, or some other IP.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

WorldClient Changes

End-to-end Email and Attachment Encryption

The WorldClient theme is now equipped with support for end-to-end email and attachment encryption through Virtru. To enable this feature, the WorldClient user must switch to the WorldClient theme, go the the Options » Compose page, and click **Enable Virtru**. This causes a button to appear on the Compose page that the user can click to encrypt his or her email before sending. This is an easy-to-use feature that doesn't require the user to remember or save any special passwords or keys. Recipients who use a Virtru-enabled client, such as the WorldClient theme or one of Virtru's other client plugins, can open and read the encrypted messages normally, without any additional steps. Recipients without a Virtru-enabled client will see a link to view the message in a special browser-based reader.

If you wish to prevent your users from being able to use Virtru encryption within WorldClient, open the `Domains.ini` file in the `MDaemon/WorldClient` folder and add `VirtruDisabled=Yes` to the `[Default:Settings]` section, or add it to a `[<Domain>:Settings]` section if you only wish to disable it for a specific domain.

For more information, see: Email Encryption.

Contacts Improvements

LookOut Theme

- Improved distribution list editor.
- Added the Categories column to the Contact List
- Added more column-display options under Options » Columns » Contacts.
- Under Options » Personalize » Contacts, you can now adjust the length of time you must hover the pointer over a contact in the Contact List before the Contact Info Preview will appear. You can also disable the Contact Info Preview.

Other Themes

- Added the ability to print individual contacts in Lite, LookOut, and WorldClient themes.

Other WorldClient Changes

- RPost is now disabled and the option is not visible to users by default. If you wish to make the RPost option available to all of your WorldClient users, open the `Domains.ini` file in the `MDaemon/WorldClient` folder, locate the `[Default:Settings]` section, and add `RPostEnabled=Yes` to that section. If instead you wish to make it available to a specific domain's users, add the key to that relevant `[<domain>:Settings]` section (e.g. `[example.com:Settings]`).
- When editing a Note or Task in the WorldClient theme, you can now click a button on the editor's toolbar to open the item in a new window.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

New in MDaemon 14.5

New Look For MDaemon Remote Administration

MDaemon's Remote Administration 251 interface received a major update, giving it a more modern look and feel. Additionally, new menus were utilized and several others were relocated to align Remote Administration more closely with MDaemon's layout, and "Mobile Device Management" is now a top-level menu item for easier access. Finally, there is now full context-sensitive help available via the Help link in the top right corner of each page.

DMARC

MDaemon Pro now supports Domain-based Message Authentication, Reporting & Conformance (DMARC), which is a specification designed to help reduce email message abuse, such as incoming spam and phishing messages that misrepresent their origins by forging the message's `From:` header. DMARC makes it possible for domain owners to use the Domain Name System (DNS) to inform receiving servers of their DMARC policy, which is how they want those servers to handle messages that purport to be sent from their domain but cannot be authenticated as having actually come from it. This policy, which is retrieved by the receiving server via a DNS query while processing the incoming message, can state that the server should quarantine or reject messages that do not align with the policy, or take no action at all (i.e. let the message proceed normally). In addition to the policy, the domain's DMARC DNS record can also contain requests for the server to send DMARC reports to someone, outlining the number of incoming messages purporting to be from that domain and whether or not they passed or failed authentication, and with details about any failures. DMARC's reporting features can be useful for determining the effectiveness of your email authentication procedures and how frequently your domain name is being used in forged messages.

Under the Sender Authentication section of the Security Settings dialog, there are three screens for configuring MDaemon's DMARC verification and reporting features: DMARC Verification 462, DMARC Reporting 464, and DMARC Settings 453.

For more information on this configuring and using this new feature, see: DMARC 455.

ActiveSync Supports Server-side Mail Search

MDaemon's ActiveSync server now supports searching messages on the server. Please refer to your ActiveSync client's documentation to find out if it supports this feature and how to use it. The search indexes are stored on the server in the folders being searched, in files named `SrchData.mrk` and `SrchIndex.mrk`. Server-side search support requires MDaemon Pro and active ActiveSync Software License Renewal Coverage.

Improved Mailing List Engine

The mailing list engine has several improvements:

- All of the header manipulation options have been moved from the Settings screen to their own new Headers 192 screen, and the options were reworked and reorganized.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

- Support for DMARC was added, which allows lists to handle incoming messages from domains with restrictive DMARC policies.
- Mailing Lists now support List-ID (RFC 2919), allows you to enter a short description for your mailing list which is included in the List-ID message header. This description is optional and if not provided the List-ID header will contain just the list identifier by itself. An example header with a description looks like this: List-ID: "Discussion of the current MDaemon Beta" <md-beta.altn.com>. An example without a description looks like this: List-ID: <md-beta.altn.com>. The email address of the mailing list itself is used as the list's unique identifier (note that the "@" is changed to a "." character to safely comply with the specification). The List-ID header is stripped from incoming messages sent to local mailing lists but not from incoming messages sent to local users from outside mailing lists.
- The List-ID specification is now supported via a new option on the Settings 189 screen. Enter a short description of your mailing list and it will be added to the `List-ID:` header included in messages that are sent to the list. The description and the list's identifier will be included in the header (e.g. `List-ID: "Frank's personal mailing list" <MyList.example.com>`).
- On the Moderation 202 screen there are new options to support Mailing List URLs. MDaemon can add to mailing list messages any of the six header fields outlined in RFC 2369: *The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields*. The six headers are: List-Help, List-Subscribe, List-Unsubscribe, List-Post, List-Owner, and List-Archive. If you wish to use any of these headers to the list's messages, enter the desired header value into any of the fields provided.
- Using the new Reminders 198 screen, you can set MDaemon to send monthly subscription reminders to the list. There is a text area provided for you to enter the contents of the message, and you can use the provided macros to add variable data to the message, such as the name of the list and the member's email address. Additionally, messages are sent as text/html so that you can use HTML code in the message if you prefer.

Improved SMTP Server

There have been significant enhancements made to MDaemon's SMTP server:

- Support for RFC 3463: Enhanced Mail System Status Codes has been added. These codes allow for much finer grained reporting and automation. As a result of this nearly all of MDaemon's SMTP server protocol strings have been changed to include the enhanced codes. Further, the way codes are stored and retrieved was simplified and modernized. Additionally, Support for RFC 2034: SMTP Service Extension for Returning Enhanced Error Codes was also added. Consequently, a new ESMTP capability called `ENHANCEDSTATUSCODES` was added and will be declared to other servers during the SMTP transaction.
- Support for RFC 3464: An Extensible Message Format for Delivery Status Notifications and RFC 6522: The Multipart/Report Media Type for the Reporting of Mail System Administrative Messages has been added. This completely overhauls MDaemon's DSN reporting. All of the old code and behavior related to this has been removed and replaced. With these changes, MDaemon's DSN

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

system now fully complies with industry standards and will properly interoperate with automation tools and other MTAs. The format of the DSN has radically changed and now rigidly complies with the specifications. This means that delivery warning messages and delivery failure messages now fall under the control of these RFCs and are no longer accessible to administrators for customization. This required several changes to the DSN Settings 661 screen. See the MDaemon 14.5 Release Note for more information about these changes.

- Support for RFC 3848: SMTP and LMTP Transmission Type Registration has been added. This governs the value of the "WITH" clause in Received headers. This means you'll see "ESMTP" for unauthenticated non-SSL sessions, "ESMTPA" for authenticated sessions, "ESMTPS" for SSL sessions, or "ESMTPSA" for authenticated & SSL sessions. Values of "MULTIPOP" and "DOMAINPOP" are MDaemon specific and will continue to be used even though they don't appear in the IANA registry.

Improved Sender Authentication

There were a number of improvements made to MDaemon's sender authentication features:

- Updated MDaemon's Sender Policy Framework (SPF) implementation to the latest specification (RFC 7208). See the MDaemon 14.5 Release Note for complete details on these changes.
- Updated MDaemon's implementation of RFC 7001: Message Header Field for Indicating Message Authentication Status. This is the latest specification governing the `Authentication-Results` header. This caused several changes to the format of the header, and it looks much different now. `PTR`, `HELO`, and `MAIL` reverse lookups now use the ABNF from RFC 7001 (i.e.. iprev and policy.iprev for `PTR`, `HELO`, and `MAIL` with comment text as the differentiator).
- Implemented RFC 6212: Authentication-Results Registration for Vouch By Reference Results. When multiple VBR hosts are used there will now be multiple VBR sections in Authentication-Results.
- Implemented RFC 6008: Authentication-Results Registration for Differentiating among Cryptographic Results. This included documenting the results of each DKIM signature in an industry standard way. Previously, MDaemon did not document all signature results and what it did document was not in industry standard form. When multiple DKIM signatures are used there will now be multiple DKIM sections in Authentication-Results.
- A new option was added to VBR Certification 471, which will force VBR checks even for incoming messages that lack the VBR-Info header.
- There have been several changes and improvements to DKIM. MDaemon's DKIM 446 implementation was updated to the latest specification (RFC 6376). Options for including header and body canonicalized data in DMARC failure reports were added to the DMARC Settings 468. Authentication-Results header now includes the results of ADSP processing where relevant as per RFC 5617. And several changes were made to the DKIM Settings 453 screen. See the MDaemon 14.5 Release Notes for more details the DKIM changes.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

WorldClient Improvements

MDaemon 14.5 includes a variety of improvements and enhancements to WorldClient's themes. See WorldClient's online Help and the MDaemon 14.5 Release Notes for more information about what's new in WorldClient.

New in MDaemon 14.0

ActiveSync Improvements

- ActiveSync WhiteList and BlackList now support wildcards. (new in 14.0.1)
- MDaemon's ActiveSync server now supports other users' shared folders 87 in addition to personal and public folders. The behavior of any client accessing shared folders via the ActiveSync protocol can vary. While MDaemon's ActiveSync implementation supports Email, Events, Contacts, Tasks and Notes, not all device clients are capable of handling this data. This feature requires MDaemon Pro and active ActiveSync Software License Renewal.
- ActiveSync User Agent protocol restrictions can now be set using the entire value, not just the portion preceding the forward slash.

Inline Image Support in HTML Signatures

MDaemon's HTML Signature 83 controls now support inline images by using the `$ATTACH_INLINE:path_to_image_file$` macro.

For example:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

You can also insert inline images via Remote Administration's HTML editor. See, *Inline Image Support in Signatures* in the Remote Administration section below.

WorldClient Changes and Improvements

ComAgent in Now WorldClient Instant Messenger (New in 14.0.1)

ComAgent is now called WorldClient Instant Messenger 225, and within WorldClient the in-browser ComAgent Chat feature it is simply referred to as Instant Messenger or instant messaging.

New WorldClient Theme (requires MDaemon Pro)

In response to customer requests for a new browser-based email client, WorldClient has a new signature theme called *WorldClient*. It is designed to have a clear, modern interface, maintaining a good balance between simplicity-of-use and breadth of features, incorporating numerous design elements from popular consumer and business browser-based email clients. Although it doesn't have every feature that is available in the LookOut theme, it is equipped with an extensive and carefully selected set that should serve most users well. The *WorldClient* theme requires at least Internet Explorer

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

9 or the latest version of Mozilla Firefox, Safari, or Chrome.

The WorldClient theme is now the default theme for new installations. When updating, the installer will ask if you want to change your default to this new theme.

Side-by-Side Calendars

LookOut and the *WorldClient* theme have a new side-by-side calendar view. This makes it possible for you to view multiple calendars side by side.

New Compose Options

- The Compose page's HTML compose editor has been updated to a newer version that is compatible with Internet Explorer 11.
- You can now insert inline images into messages by using the new HTML tools on the Compose page.
- The English and English-UK spell check dictionaries have been updated.

Simple Theme Renamed

The *Simple* theme has been renamed to *Lite*.

WebAdmin Changes and Improvements

WebAdmin is Now MDaemon Remote Administration (New in 14.0.1)

WebAdmin is now simply referred to as MDaemon's remote administration interface, or Remote Administration, in the MDaemon GUI and elsewhere. This is to help users better understand that the Remote Administration component is an integrated feature of MDaemon rather than a separate product.

Inline Image Support in Signatures

Added support for several ways to insert inline images into the Default 83 and Domain 138 signatures:

- On the Signature/Footer screen in Remote Administration, click the "Image" toolbar button in the HTML editor and select the upload tab
- On the Signature/Footer screen in Remote Administration, click the "Add image" toolbar button in the HTML editor.
- Drag and drop an image into the Signature/Footer screen's HTML editor with Chrome, FireFox, Safari, or MSIE 10+
- Copy and paste an image from the clipboard into the Signature/Footer screen's HTML editor with Chrome, FireFox, MSIE 11+

Improved Administration

Global Administrators can now:

- Configure Outbreak Protection settings

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

- Configure server-wide Autoresponder settings
- Freeze/Unfreeze mail queues
- Manage Queues
- Administer WorldClient server settings

Other Remote Administration Improvements

New in 14.0.1

- Added mailbox reports for quotas, for mailbox size and message count.
- Added Manual Learn button to Spam Filter Bayesian Classification section.
- Log files can now be viewed in a new window.
- Logos and color scheme updated.

New in 14.0.0

- Remote Administration's Account Manager now displays icons for Outlook Connector and ActiveSync users.
- Added *Return port settings to defaults* option.

Additional Features and Changes

MDaemon 15.5 has many new features and changes. See `RelNotes.html` located in MDaemon's `\Docs\` subfolder for a complete list of all new features, changes, and fixes to MDaemon from the previous version.

New in MDaemon 13.6

Simple Message Recall (New in 13.6.1)

MDaemon Pro now has a simple message recall system that can be enabled and configured on the new Message Recall 721 screen, located on the Server Settings dialog. Using this system you can choose to delay incoming messages sent by authenticated local users for 1 to 15 minutes. During that delay period the messages are simply left in the inbound mail queue. This provides a short period during which a user can attempt to stop a message from being delivered. Once the delay period expires the message is delivered normally. The message recall feature is disabled by default. When the feature is enabled, the default delay period is 1 minute.

To recall a message a user can simply log in to WorldClient and click the *Recall* button that will be displayed when viewing a recently sent message in the Sent Items folder. If clicked before the recall time limit expires, WorldClient will send a RECALL message to MDaemon. Alternatively, the user can go the the Sent Items folder in his mail client, locate the message he wishes to recall, and then "Forward as Attachment" the message to the `mdaemon@example.com` system account, using "`RECALL`" as the message's Subject. Another alternative is to view the message's headers, copy the `Message-ID` header value (the part to the right of the "`Message-ID:`" string), create a new message and place "`RECALL`" plus the message ID value in the subject. If both

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

alternatives are used within the same recall message, only the message ID option will be used.

Regardless of the chosen recall method, MDaemon will send an email back to the user, saying whether or not the recall was successful. When a message is successfully recalled, MDaemon deletes the message from the inbound queue as if it had never been sent. All recall processing is logged to MDeamon's Routing log.

Enhanced Reporting for WebAdmin

A Statistics Log screen was added to the Logging dialog, with options for controlling the statistics log file and a new SQLite database file used for logging statistical information about MDaemon's activity. This database is used by WebAdmin's new Reports feature and contains data on MDaemon's bandwidth usage, number of inbound and outbound messages, spam statistics, and the like. By default this database is stored in the "MDaemon\StatsDB" folder and 30 days worth of data is saved, but you can adjust how long to keep the data if you wish to retain more or less than the default 30 days. Data older than the designated limit will be removed during the nightly maintenance process. You can also specify how often MDaemon will compact the database to conserve space.

The Reports page in WebAdmin uses this database to generate a variety of reports available to Global administrators. For each report, data may be generated for several predefined date ranges, or the admin may specify a custom date range. Administrators can choose from the following reports:

- Enhanced bandwidth reporting
- Inbound vs. Outbound messages
- Good messages vs. Junk messages (percentage of email that is spam or a virus)
- Inbound messages processed
- Top recipients by number of messages
- Top recipients by message size
- Outbound messages processed
- Top spam sources (domains)
- Top recipients of spam
- Viruses blocked, by time
- Viruses blocked, by name

ActiveSync Server Now Supports Public Folders (requires MDaemon Pro)

ActiveSync Services for MDaemon now support MDaemon's public folders in addition to mailbox folders. The behavior of any client accessing public folders via the ActiveSync protocol can vary. While MDaemon's ActiveSync implementation supports Email, Events, Contacts, Tasks and Notes, not all device clients are capable of handling this data. Public folder access can be controlled at the user, domain, and server levels.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

There is a new global option on the Public & Shared Folders 87 screen (and mirrored on the ActiveSync » Settings 312 screen) for controlling whether or not ActiveSync users will be able to access their public folders from their devices. There are corresponding options on the Domain Manager 140 and Account Editor 525 that can be used to override the global setting for specific domains and users, respectively.

New in MDaemon 13.5

Improved ActiveSync for MDaemon (Requires MDaemon Pro)

The ActiveSync server 276 now supports additional ActiveSync protocol versions: 12.1, 14.0, and 14.1. This provides ActiveSync support for a wider variety of devices and applications, including Outlook 2013. This change provides new ActiveSync policy capabilities and improves overall device management. ActiveSync for MDaemon is a separately licensed product with a free trial period, and it can be purchased from www.altn.com or your local distributor/reseller.

Additional ActiveSync changes include:

- The Policies 284 screen has been redesigned and supports many new ActiveSync policy options.
- Settings 312 has a new control to specify the number of days that an ActiveSync device 297 can go without connecting to MDaemon before it will be forgotten. When MDaemon forgets a device, its configuration and access settings are discarded. If the device ever connects again, MDaemon will respond as if it is a new device that has never been used on the server. It will be forced to reprovision if a policy is in place for the domain 292, perform an initial folder sync, and re-sync all subscribed folders. This option can help keep your server free from maintaining information for old and unused devices. The option is set to 31 days by default.
- The Integrated Accounts screen was redesigned and renamed to "Devices 297".
- There is now a White List and Black List for ActiveSync. The White List is used to exempt specific devices or device operating systems from provisioning, or policy 284 restrictions. The Black List is used to restrict devices or device operating systems from accessing MDaemon's ActiveSync server. For both lists you can create entries based on *Device ID*, *Device Type*, and *Device OS*.
- The new Restrictions 278 screen allows you to specify User Agent and Device Type values and restrict devices matching those values to specific versions of ActiveSync.

Improved Attachment Linking (Requires MDaemon Pro)

- For accounts configured to use the Attachment Linking 262 feature, it can now be used for outbound messages as well, with a new option on the Account Editor's Attachments 539 screen for enabling the new feature on a per-user basis. When the user sends an email, Attachment Linking will extract the file, store it, and replace it with a URL to the file.
- You can now specify the maximum number of days that any attachment will be stored. As part of the daily cleanup event, MDaemon will remove from the root

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

attachment folder and its subfolders any file found to be older than the specified number of days. This only works when you are using the default root attachment folder: `<MDaemonRoot>\Attachments\`. It does not work if you customize the attachment folder to point elsewhere.

- You can now specify a minimum size below which attachments are not extracted. Using this option you can configure MDaemon to ignore small attachments, extracting only larger ones.
- Attachment Linking will try to use the file name provided in the MIME headers, if one is present. If the file name is longer than 50 characters then only the last 50 characters will be used. If the file name is missing an extension, "`.att`" will be appended.

Public Folder Manager (Requires MDaemon Pro)

MDaemon now has a Public Folder Manager 218 under the Setup menu, to help you administer your Public Folders more efficiently. The Public & Shared Folders 87 screen, however, is still located on the Server Settings dialog for managing your global settings.

Improved Domain Manager

- The Domain Manager 121 has been redesigned. It now displays several screens for each domain instead of having everything on a single screen, and there are better options for creating, deleting, and renaming domains. Further, many domain specific functions have been moved there and consolidated from other places in the UI. As a result of this you will no longer find default domain related settings on the Server Settings dialog. You can still designate a Default Domain via a button on the Domain Manager, but that designation is only needed in a few circumstances, such as any time the server engines cannot determine a more appropriate domain to use in a given processing context (which should be almost never).
- Domain Signatures (both plain text and html) were combined onto a single screen called Signatures 138 and moved to the Domain Manager. The Server Settings dialog contains a similar screen called Default Signatures 83, used for Domains without a designated Domain Signature.
-
- When you have configured MDaemon's Delivery 50 options to send some messages to a Smart Host, you can now specify different Smart Host settings on a per-domain basis using the Domain Manager's Smart Host 125 screen. When no Smart Host has been specifically designated for a domain, the default Smart Host will be used.

Group and Template Managers

MDaemon now contains both Group and Template Managers. The Group Manager 576 helps you more easily manage groups. It is used to create account Groups and manage which accounts belong to them. Groups have a number of different uses and functions. For example, using the Group Properties 577 screen you can assign an account template to a Group, allowing you to control a variety of account settings for group members.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

You can also control whether or not group members have access to ComAgent and instant messaging. Further, the Content Filter supports groups, allowing you to create rule conditions based on whether or not a message sender or recipient is a member of a specific Group. Finally, for Shared Folders you can assign Access Control List rights to specific Groups, meaning all members of that Group will share those access rights. You can add accounts to a Group from both the Group Manager and from each user's Mail Folder & Groups 524 screen.

With the Template Manager 580 you can create and manage Account Templates, which are named sets of account settings that can be assigned to specific Groups. Any account belonging to one or more of those groups will have the designated account settings locked, being controlled only by the assigned templates rather than by the Account Editor. The categories of account settings that a template will control are designated on each template's properties 582 screen, which is reached by double-clicking the template's name. Further, there is a special template called "*New Accounts*" that replaces the old New Account Defaults screen. This special template is applied to all new accounts when they are created. Rather than locking and controlling certain account settings like other templates, *New Accounts* is used simply to designate the initial settings for new accounts. Those initial settings can then be changed normally by using the Account Editor to edit individual accounts.

Colorized Session Logs 119

On MDaemon's user interface 41, the tabs that display Routing, SMTP-in, SMTP-out, IMAP, POP, MultiPOP, and DomainPOP activity can now be colorized to help visually separate events during a session. This features is disabled by default, but can be enabled via the "*Use colors when displaying mail session logs*" option located at: Logging » Settings 116 and Preferences » UI 344. The default text colors can be changed by editing the `[Colors]` section of the `LogColors.dat` file. See the Logging Settings 119 page for more information and a list of the default colors.

Improved Active Directory Monitoring (Requires MDaemon Pro)

Active Directory monitoring has been improved to periodically query Active Directory and keep all public contact records updated with the most recent information stored. Common fields like an account's postal address, phone numbers, business contact information, and so on will be populated into their public contact record, and this data will be updated any time it is changed in Active Directory. Numerous contact record fields will be monitored in this way. For a complete list of which public contact record fields can be mapped to Active Directory attributes, see the contents of the ActiveDS.dat file in MDaemon's `\app\` folder. Also, you do not need to enable full Active Directory account monitoring to take advantage of this. A new option on the Active Directory Monitoring 608 screen allows you to enable this feature separately from full Active Directory account monitoring.

This feature will create contact records on the fly if they don't already exist, and it will update contact records that do exist. Further, please note that it will overwrite any changes you make outside of Active Directory. Contact record fields that are not mapped are left unaltered. Therefore any existing data that is not subject to this process will not be altered or lost. Finally, MDaemon accounts that are set to private 573 are not subject to having their contact records created or updated.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Performance Counters

Windows Performance Counters have been implemented to allow monitoring software to track MDaemon's status in real time. There are counters for the number of active sessions for the various protocols, number of messages in the queues, server active / inactive states, MDaemon up time, and session and message statistics.

To use the performance counters, start System Monitor by going to Control Panel | Administrative Tools | Performance, or by running "perfmon". These are 32-bit counters so on 64-bit machines you must run "mmc /32 perfmon.msc". Click on Add Counters, select the MDaemon performance object, then select and Add the counters that you want to see. To see the performance counters from MDaemon running on another machine you must have the "Remote Registry" service enabled and access through any firewalls.

See:

Introduction 12
Upgrading to MDaemon 15.5.0 31
MDaemon's Main Display 40

1.4 Upgrading to MDaemon 15.5.0

Below is a list of special considerations and notes that you may need to be aware of when upgrading to MDaemon version 15.5.0 from a previous version.

- The daily quota report now includes a column showing the last date and time the account was accessed (via IMAP, POP, WorldClient, etc). This required a change to the `QuotaReport.dat` template file. Your old file was saved as `QuotaReport.dat.old` in case you have customized it. If so, you may want to similarly customize the new template file.
- The default setting for *Use colors in UI logs* was changed from disabled to enabled. If you don't wish to use colorized logs 119 you can change the setting at: Preferences » UI 344.

Version 15.0.0

- Account Hijack Detection 486 is now enabled by default.
- Dynamic Screening 482 has changed. The "Watch accounts" checkbox was redundant and therefore removed. The options to freeze accounts and email the postmaster were made into a separate checkboxes, and you can now designate the sources that will trigger the email: SMTP, IMAP, or POP. As in previous versions, this email is not sent when the account in question is already frozen. Further, the Dynamic Screening settings were reverted to installation defaults, therefore you should check them if you prefer a non-default configuration. Finally, the WorldClient-related options were moved to their own Dynamic Screen 237 page under WorldClient (web mail).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Version 14.5.0

- On the Preferences » Headers 352 screen, the options: "*Hide local IPs when processing message headers*" and "*...also hide LAN IPs*" have been deprecated and removed. They have been replaced by a single option that hides reserved IP addresses: "*Hide reserved IPs when creating message headers*." This option is enabled by default and prevents reserved IP addresses from appearing in certain MDaemon created message headers. Reserved IP addresses are as defined by various RFC's and include: `127.0.0.*`, `192.168.*.*`, `10.*.*.*`, and `172.16.0.0/12`. If you also wish to hide your domain IPs (including LAN domains) from the headers then you can set the following switch in MDaemon's `app\MDaemon.ini` file manually: `[Special] HideMyIPs=Yes` (default is `No`).
- The option "*POP3, IMAP, and WorldClient passwords are case sensitive*" has been deprecated and removed from Preferences » Miscellaneous 354. Passwords are now always case-sensitive. Allowing otherwise breaks security best practices and is incompatible with hash-based authentication mechanisms (APOP, CRAM-MD5) and secure (hash-based) password storage. As a result of this, some of your users may need to update their password in their mail client.
- The SPF cache file 444 now caches a domain's actual SPF policy record taken from DNS rather than the final result of SPF processing. Your old `SPFCache.dat` file can not be migrated and was therefore renamed to `SPFCache.dat.old` in case it contains settings you need to refer to. You can delete `SPFCache.dat.old` at any time.
- The HashCash feature was removed. It was an outdated feature that was never widely used.
- All support for the now obsolete Sender-ID feature was removed.
- All support for the original DomainKeys message authentication system has been removed. DomainKeys is obsolete and has been replaced by the acceptance and adoption of DKIM 446.

Version 14.0.1

- WebAdmin has been renamed to MDaemon Remote Administration.
- ComAgent has been renamed to WorldClient Instant Messenger.

Version 14.0.0

- The product registration system has been updated to utilize a digitally signed XML based license file. This approach allows for greater flexibility, and will enable ALT-N to offer new innovative purchasing and renewal options. The installation process will automatically download the license file. Product activation has been replaced by a scheduled mechanism that will update the license file on a periodic basis. The system is able to accommodate temporary connectivity outages, but communication with the licensing service is required for continued use of the product.
- The new *WorldClient* theme is now the default theme for new installations. When

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

updating, the installer will ask if you want to change your default to this new theme.

- WorldClient's Simple theme has been renamed to Lite. MDaemon Lite now uses this theme in WorldClient.
- The Standard theme is no longer included in new installations of MDaemon, but it will still be available as a separate download. If you are updating and the Standard theme is already installed, it will not be removed.

Version 13.6.1

- The default settings for two SMTP authentication related values have changed. The option to require SMTP authentication when mail is from local accounts and the option to require authentication credentials to match that of the email sender are both now enabled by default. If you wish to disable either of these options, they are located on the SMTP Authentication 442 screen.
- An option was added to Preferences » Headers 352 to hide MDaemon's software version and other identifying information when creating Received headers or responding to various protocol requests. The option is disabled by default. As part of this process, MDaemon's Received header construction was simplified and no longer includes extraneous data. Also, the following undocumented MDaemon.ini settings were removed: `[Special] SecureReceivedHeaders=Yes/No` and `[Special] ReceivedHasAuthedUser=Yes/No`.
- The STARTTLS Required List 500 is now also applied to the `MAIL FROM` value during an SMTP session (in addition to the `EHLO` and `IP`). If MDaemon receives a `MAIL` command followed by an email address that is on the STARTTLS Required List during a session that has not been secured, then the `MAIL` command will get a "`454 STARTTLS Required`" response.

Version 13.6.0

- MDaemon Standard has been renamed to MDaemon Lite.
- The trial period for MDaemon, SecurityPlus, Outlook Connector, and ActiveSync has been reduced from 60 days to 30 days.

Version 13.5.2

- The way smart hosts are used has changed. In the past the smart host for a domain was only used when the Delivery routing option 50 to send mail to domain smart hosts was enabled. This made it impossible to use smart hosts for only some domains while simultaneously using standard direct delivery for others. Now if a smart host is configured and enabled for a specific domain under the Domain Manager 125, then that domain's outbound mail will be routed to the smart host regardless MDaemon's main delivery setting. So, now it is possible to specify and use smart hosts for some (and not necessarily all) of your domains. **Please note that use of smart hosts had to be reset to OFF for all domains due to this change. So, if you want to enable smart hosts for one or more domains use the domain manager 125 to do so.**
- The WebAdmin log rollover and storage options have changed. WebAdmin will

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

now rollover its logs on the same schedule as MDaemon (F2 | Logging in the MDaemon GUI). Weekly and Monthly rollovers are no longer supported. Additionally, new installs starting with this release will have their WebAdmin logs stored in the same location as the MDaemon logs (\MDaemon\Logs by default). Lastly, the WebAdmin-specific logging options that remain have moved under the general Log Options menu in WebAdmin.

Version 13.5.0

- Please note that MDaemon's BlackBerry Enterprise Server does not (and can not) work with BlackBerry OS 10 devices. BlackBerry OS 10 devices are managed through MDaemon's ActiveSync server or with different management tools obtained directly from BlackBerry. MDaemon's BlackBerry Enterprise Server management features are for devices running BlackBerry OS 7 or earlier.
- The operation of SSL & TLS » STARTTLS Required List 500 has changed. Hosts and IP addresses listed here will now require TLS on both incoming and outgoing connections from any host or IP on the list. In the past, the list only applied to outgoing connections. Also, IPs listed here can now be specified in CIDR notation.
- Prior to 13.5.0, public folders could not be deleted automatically when a domain was deleted. Now there is a new option on the Public & Shared Folders 87 screen to control this. Enable the "*Delete domain public folders when domain is deleted*" option if you wish to delete a domain's public folders as well. Enabling this option is recommended, but in order to preserve existing behavior it is disabled by default.
- When 13.5.0 is started for the first time it will perform a one-time migration of account settings from `WEBACCES.DAT` into the accounts' `HIWATER.MRK` file, which is a more appropriate place for these configuration settings. The `WEBACCES.DAT` file is no longer used and will be removed as part of this migration process. Further, the Web Services 587 settings on the *New Accounts* template only apply to newly created accounts, not to existing accounts. A new "*Apply installation defaults*" button reverts all the settings on this page to installation defaults
- The content of the `NoComd.dat` file is obsolete. Depending on your configuration, this file was emailed like an autoresponder to anyone who submitted an MDaemon command email that failed to contain valid commands for MDaemon to process. The content of the file contained instructions on how to ask for help, which were also obsolete. A new `NoCommand.dat` file has been created which no longer contains this errant instructions. If you would like to provide instruction to non-local users on (for example) how to send a SUBSCRIBE or UNSUBSCRIBE command email you can easily modify the `NoCommand.dat` file to do so. If you have previously modified the `NoComd.dat` file you can move your modifications into `NoCommand.dat` from the backup of `NoComd.dat` which was created as part of the installation process or from a backup created by the nightly config file backup feature.
- MDaemon no longer supports extraction of attachments into an account's FILES folder. This folder was rarely accessible. Instead, this option extracts attachments into the account's Documents IMAP folder which is accessible via WorldClient. Each account's FILES folder will be left in place in case there are files there that should not be deleted. However, no further use of this folder is

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

made by MDaemon. As part of this, the $FILEDIR$ macro was removed.

- The format of log file lines in colorized logs 119 has changed to include a two-digit color code in each line immediately following the time-stamp.
- It is possible to accidentally configure a valid account to receive bounces from mailing lists in such a way as to cause the list pruning operation to delete the account's other (non-list) related mail. To help prevent this we have updated the documentation with warnings and have reversed the default settings for two existing options located at Mailing List Settings 183. "*Mailing list pruner deletes messages that it can't parse*" is now disabled by default, and "*Mailing list pruner saves messages that cause list member removal*" is enabled by default. Please set these options to how you want your system to behave. For more information see: Enhanced List Pruning 191.
- MDaemon will no longer bounce messages on a 5XX error from your smart host if one or more of the MX hosts from the receiving domain returned a temporary error earlier in the delivery session. This is on the theory that maybe one of the receiving domain's servers will correct itself before the next queue run. However, it is an indication of a bad site configuration if you are using a smart host and that smart host refuses to accept mail from your MDaemon server. It is expected that this will not ordinarily be the case. A new option was added to Server Settings » Delivery 50 called "*Bounce message on 5XX error from smart host*" which defeats this mechanism and causes the message to go ahead and immediately bounce. If the message is not bounced it becomes part of the standard retry queue mechanism. If all of the receiving domains MX hosts return 5XX errors and the smart host returns 5XX errors then the message has nowhere else to go and is bounced regardless of any other settings.

See:

Introduction 12
New in MDaemon 15.5 15
MDaemon's Main Display 40

1.5 Getting Help

Support Options

Support is a vital part of the total Alt-N Technologies customer experience. We want you to get the most from our products long after the initial purchase and installation and we are dedicated to ensuring that any issues are resolved to your satisfaction. For the latest Customer Service information, Technical Support Options, Self-support Resources, Product Information, and more, visit the Alt-N Technologies support page at: www.altn.com/support/

MDaemon Beta Testing

Alt-N Technologies maintains active beta testing teams for our products. If you would like information about joining the MDaemon beta team, send a message to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

MDaemonBeta@altn.com.

The Beta Team is for those who wish to acquire Alt-N software before its general release and aid in its testing; it is not a technical support alternative. Technical support for MDaemon will only be provided through those methods outlined at: www.altn.com/support/.

Contact Us

Hours of Operation
M-F 8:30 am - 5:30 pm Central Standard Time
Excludes weekends and U.S. holidays
Customer Service or Sales
U.S. Toll Free: 866-601-ALTN (2586)
International: 817-601-3222
sales@helpdesk.altn.com

Technical Support
www.altn.com/support/

Training
training@altn.com

Business Development/Alliances
alliance@altn.com

Media/Analysts
press@altn.com

Channel/Reseller Inquiries
Please refer to the Channel Partner page for additional information.

Corporate Headquarters

Alt-N Technologies, Ltd.
4550 State Highway 360, Suite 100
Grapevine, Texas 76051
U.S. Toll Free: 866-601-ALTN (2586)
International: 817-601-3222
Fax: 817-601-3223

Trademarks

Copyright © 1996-2015 Alt-N Technologies, Ltd. Alt-N®, MDaemon®, and RelayFax® are trademarks of Alt-N Technologies, Ltd.

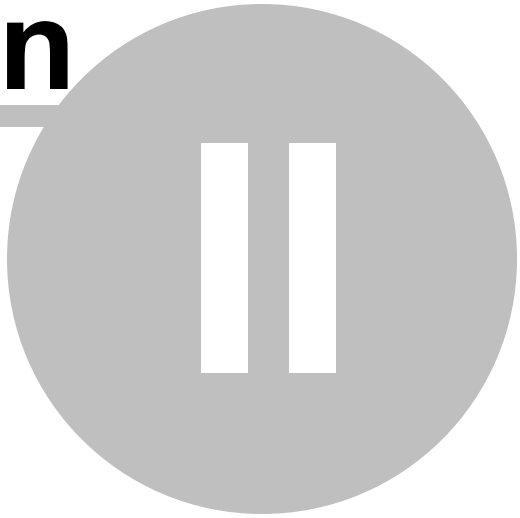
BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™, BBM™ and related trademarks, names and logos are the property of Research In Motion Limited and are

registered and/or used in the U.S. and countries around the world. Used under license. Apple is a trademark of Apple Inc. Windows Mobile, Microsoft and Outlook are trademarks of Microsoft Corporation. Palm is a trademark of Palm Trademark Holding Company, LLC. All other trademarks are the property of their respective owners.

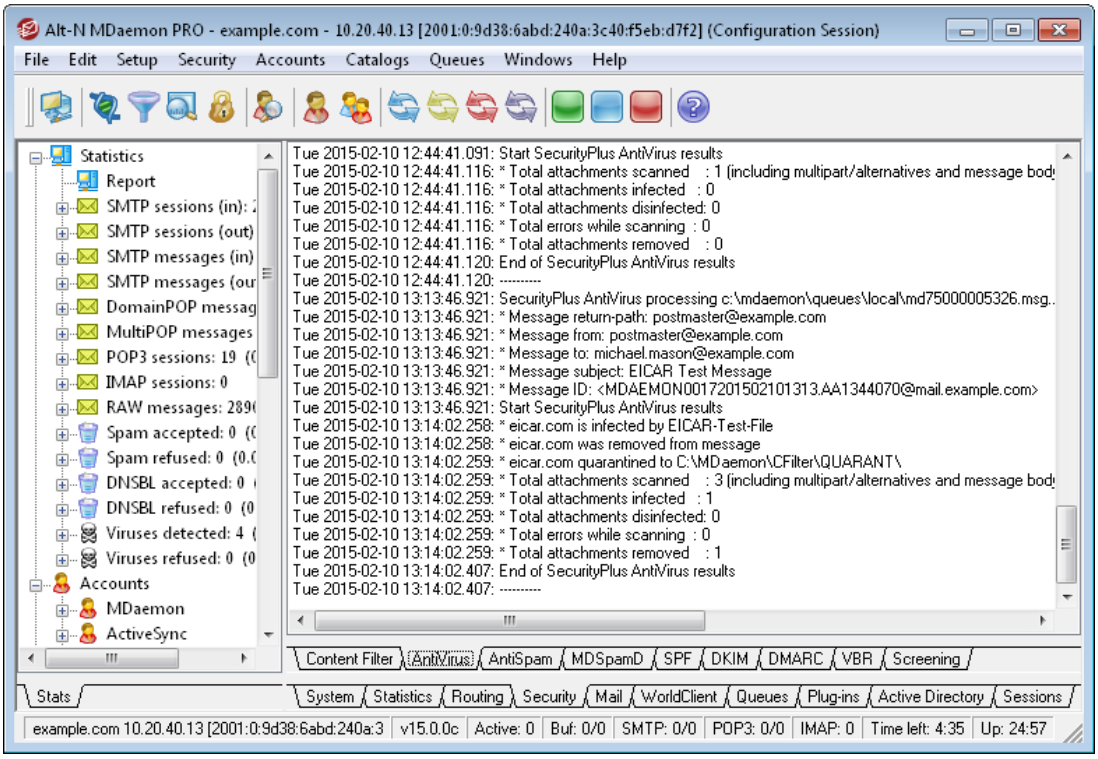
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Section



2 MDaemon's Main Display


Alt-N MDaemon PRO - example.com - 10.20.40.13 [2001:0:9d38:6abd:240a:3c40:f5eb:d7f2] (Configuration Session)
File Edit Setup Security Accounts Catalogs Queues Windows Help
Statistics
Report
SMTP sessions (in):
SMTP sessions (out)
SMTP messages (in)
SMTP messages (our
DomainPOP messag
MultiPOP messages
POP3 sessions: 19
IMAP sessions: 0
RAW messages: 289
Spam accepted: 0
Spam refused: 0
DNSBL accepted: 0
DNSBL refused: 0
Viruses detected: 4
Viruses refused: 0
Accounts
MDaemon
ActiveSync
Tue 2015-02-10 12:44:41.091: Start SecurityPlus AntiVirus results
Tue 2015-02-10 12:44:41.116: * Total attachments scanned : 1 (including multipart/alternatives and message bod
Tue 2015-02-10 12:44:41.116: * Total attachments infected : 0
Tue 2015-02-10 12:44:41.116: * Total attachments disinfected: 0
Tue 2015-02-10 12:44:41.116: * Total errors while scanning : 0
Tue 2015-02-10 12:44:41.116: * Total attachments removed : 0
Tue 2015-02-10 12:44:41.120: End of SecurityPlus AntiVirus results
Tue 2015-02-10 12:44:41.120: ----------
Tue 2015-02-10 13:13:46.921: SecurityPlus AntiVirus processing c:\mdaemon\queues\local\md75000005326.msg..
Tue 2015-02-10 13:13:46.921: * Message return-path: postmaster@example.com
Tue 2015-02-10 13:13:46.921: * Message from: postmaster@example.com
Tue 2015-02-10 13:13:46.921: * Message to: michael.mason@example.com
Tue 2015-02-10 13:13:46.921: * Message subject: EICAR Test Message
Tue 2015-02-10 13:13:46.921: * Message ID: <MDAEMON001720150210131313.AA1344070@mail.example.com>
Tue 2015-02-10 13:13:46.921: Start SecurityPlus AntiVirus results
Tue 2015-02-10 13:14:02.258: * eicar.com is infected by EICAR-Test-File
Tue 2015-02-10 13:14:02.258: * eicar.com was removed from message
Tue 2015-02-10 13:14:02.259: * eicar.com quarantined to C:\MDaemon\CFilter\QUARANT\
Tue 2015-02-10 13:14:02.259: * Total attachments scanned : 3 (including multipart/alternatives and message bod
Tue 2015-02-10 13:14:02.259: * Total attachments infected : 1
Tue 2015-02-10 13:14:02.259: * Total attachments disinfected: 0
Tue 2015-02-10 13:14:02.259: * Total errors while scanning : 0
Tue 2015-02-10 13:14:02.259: * Total attachments removed : 1
Tue 2015-02-10 13:14:02.407: End of SecurityPlus AntiVirus results
Tue 2015-02-10 13:14:02.407: ----------
Content Filter AntiVirus AntiSpam MDSpamD SPF DKIM DMARC VBR Screening
Stats
System Statistics Routing Security Mail WorldClient Queues Plug-ins Active Directory Sessions
example.com 10.20.40.13 [2001:0:9d38:6abd:240a:3 v15.0.0c Active: 0 Buf: 0/0 SMTP: 0/0 POP3: 0/0 IMAP: 0 Time left: 4:35 Up: 24:57

MDaemon's main graphical user interface (GUI) gives you important information regarding MDaemon's resources, statistics, active sessions, and queued mail waiting to be processed. It also contains options for easily activating/deactivating MDaemon's various servers. The GUI's tabbed panes keep you up to date on how the server and its incoming and outgoing connections are performing.

Stats

The Stats pane is the default left pane of MDaemon's main interface. This pane contains four sections: Statistics, Accounts, Queues, and Servers.

The *Statistics* section contains statistics regarding the number of messages sent and received by MDaemon as well as statistics for POP and IMAP sessions, Spam accepted and refused, viruses, and more. These stats are counted from the time MDaemon starts, and there is a right-click shortcut menu that can be used to clear the counters.

When you click the "reset root node counters" option, all of the counters will be reset, not merely the one you right-click. Further, there is an option at Setup » Preferences » GUI that can be used to "*Preserve root node mail counters across reboots*." Otherwise they will be reset whenever the server is rebooted.

The *Accounts* section contains entries for MDaemon, Outlook Connector, and

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

ActiveSync. Each entry lists the number of accounts used and the number of accounts left, depending on your product license.

The *Queues* section contains an entry for each message queue and the number of messages (if any) that each queue contains. You can right-click on each of the queue entries to open a shortcut menu containing one or more of the following options, depending on which queue you select:

View Queue — this option switches the main pane to the Queues tab and displays the selected queue. A list of all messages the queue contains will be displayed, and you can right-click any message to open a shortcut menu containing numerous options similar to those available in the Queue & Statistics Manager such as Copy, Move, Edit, White list, and so on.

Queue and statistics manager — open the Queue and Statistics Manager to the Queue Page with the selected queue displayed.

Process Now — this option "re-queues" all messages contained in the queue and attempts to process them normally for delivery. If you attempt to process messages contained in the Holding queue, Bad queue, or the like then the messages may encounter the same errors that put them there in the first place and return them to the same queue.

Freeze/unfreeze queue — temporarily pauses processing for the selected queue, or continues the processing if it is currently paused.

Release — releases messages from the Holding Queue. MDaemon will attempt to deliver the messages regardless of errors encountered — they will not be returned to the Holding Queue even if they encounter the same errors that caused them to be moved there originally.

Re-Queue — This is available for the Holding Queue, and has the same effect as *Process Now* above.

Enable/disable queue — activates or deactivates the Holding Queue. When disabled, messages will not be moved to the Holding Queue regardless of errors encountered.

The *Servers* section contains an entry for each server within MDaemon, and each entry lists the current state of the server: "Active" or "Inactive". Listed below each server's entry is an entry for each domain (when applicable) and the port and IP address currently in use by that server or domain. The shortcut menu provides a control for toggling each server between the Active and Inactive state. When a server is inactive its icon will turn red.

Event Tracking and Logging

The default right-hand pane of the main interface contains a group of tabs that display MDaemon's current actions and the status of its various servers and resources, and they are continually updated to reflect current server conditions. Each active session and server action is logged onto the appropriate tab once each action is complete. The information displayed on these tabs is mirrored in the log files kept in the Logs directory, if you have chosen to log such activity.

The primary pane of MDaemon's GUI contains the following tabs:

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

System — at program startup, the System tab displays a log of the Initialization Process, which can alert you to possible problems with MDaemon's configuration or status. It also displays activity such as enabling/disabling any of MDaemon's various servers.

Statistics — this tab will display a server statistics report corresponding to the information contain in the various root node counters on the Stats tab in the Stats and Tools pane. If you wish to change the font or font size used for this report you can do so by editing the following keys in the MDaemon.ini file:

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

Further, at midnight each night, the Postmaster and all addresses listed on the Recipients 380 screen of the Content Filter will get a copy of this report via email. This is the same report that is generated when you use the "Status" email command listed in General Email Controls 681. If you do not wish this report to be sent, then disable the "*Send stats report to postmaster at midnight*" option located on the Miscellaneous 354 screen under Preferences.

Routing — displays the routing information (To, From, Message ID, and so on) for each message that is parsed by MDaemon.

Security — click this tab and several other security-related tabs will appear above it.

Content Filter — MDaemon's Content Filter 364 operations are listed on this tab. When a message matches the criteria of one of the Content Filter's message rules, the relevant information related to that message and the actions taken are logged here.

AntiVirus — if you have installed SecurityPlus for MDaemon 362, then all AntiVirus operations are listed on this tab.When a message is scanned for viruses, the relevant information related to that message and the action taken is logged here.

AntiSpam — displays all of MDaemon's spam filtering 401 and prevention activities.

MDSpamD — lists all activity of the MDaemon Spam Daemon 411.

SPF — displays all Sender Policy Framework 444 activities.

DKIM — lists all DomainKeys Identified Mail 446 activities.

DMARC — lists all DMARC 455 activities.

VBR — this tab displays VBR Certification 469 activities.

Screening — this tab displays Tarpitting 508 and Dynamic Screening 482 activities.

Mail — click this tab and several other mail-related tabs will appear above it.

SMTP (in) — all incoming session activity using the SMTP protocol is displayed on this tab.

SMTP (out) — all outgoing session activity using the SMTP protocol is displayed on this tab.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

IMAP — mail sessions using the IMAP protocol are logged on this tab.

POP3 — when users collect email from MDaemon using the POP3 protocol, that activity is logged here.

MultiPOP — this tab displays MDaemon's MultiPOP mail collection activities.

DomainPOP — this tab displays MDaemon's DomainPOP activity.

LDAP — displays LDAP server activity.

Minger — displays Minger 640 server activity.

RAW — RAW or system generated message activity is logged on this tab.

Outlook Connector — displays all Outlook Connector activities.

BES — displays activities related to MDaemon's BlackBerry Enterprise Server 314 support.

BIS — displays activities related to MDaemon's BlackBerry Internet Service 336 support.

WorldClient

WorldClient — displays WorldClient's mail activities.

SyncML — this tab mirrors the data contained in the SyncML log file.

ActiveSync — this tab displays ActiveSync activity.

Queues — this tab gives access to another row of tabs above it with one tab corresponding to each message queue, such as: Local, Remote, Holding, Quarantine, Bayesian Spam, and so on.

Plug-ins — displays all activities related to any MDaemon plug-ins.

Active Directory — displays all Active Directory related activity.

Sessions — click this tab and several other tabs will appear above it. These tabs display an entry for each active connection to MDaemon. Whether the connection is SMTP in or out, POP in or out, IMAP, WorldClient, or ActiveSync, information about each active session is displayed here. Double-click on an active session to display a Session Window 46, which displays the transcript of the SMTP session as it progresses.

The information displayed on these tabs has no affect on the amount of data that is actually stored in the log files. However, MDaemon does support a great deal of flexibility with regard to the amount and type of information that is logged in those files. See the Logging 109 dialog for more information on logging options.

Event Tracking Window's Shortcut Menu

If you right-click in any of the Event Tracking pane's tabs it will open a shortcut menu. Various options are provided on this menu that can be used to select, copy, delete, or save the contents of a given tab. The menu's *Print/Copy* option will open any currently selected text in Notepad, which can then be used to print the data or save it to a file.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

The *Delete* option will delete the text you have selected. The *Search* option will open a window in which you can specify a word or phrase to search for in the log files. MDaemon will search all log files for the text string and then all session transcripts containing that string will be combined into a single file and opened in Notepad for your review. A practical use of this feature would be to search for a particular Message-ID, which would provide a compilation from all the logs of all session transcripts containing that Message-ID.

The layout of the MDaemon GUI is not limited to the default positions described above. You may switch their position by clicking Windows » Switch Panes on the menu bar.

Composite Log View

Located on the Windows menu of MDaemon's menu bar is the Composite Log View option. Clicking this option will add a window to the GUI that will combine the information displayed on one or more of the main pane's tabs. Use the options on the Composite Log 111 screen of the Logging dialog to designate the information that will appear in that window.

See:

Session Window 46
Tray Icon 44
Shortcut Menu 45
Composite Log 111

2.4 Tray Icon

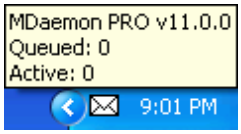
Whenever the MDaemon server is running, its icon will be visible in the system tray. However, apart from simply letting you know whether the server is running, the icon is also dynamic and will change colors based upon the current server status. The following is a list of the icon indicators:

	All okay. No mail in local or remote queues.
	All okay. Mail in local or remote queues.
	Available disk space below threshold (see Setup » Preferences » Disk 349).
	Network is down, dialup failed, or disk is full.

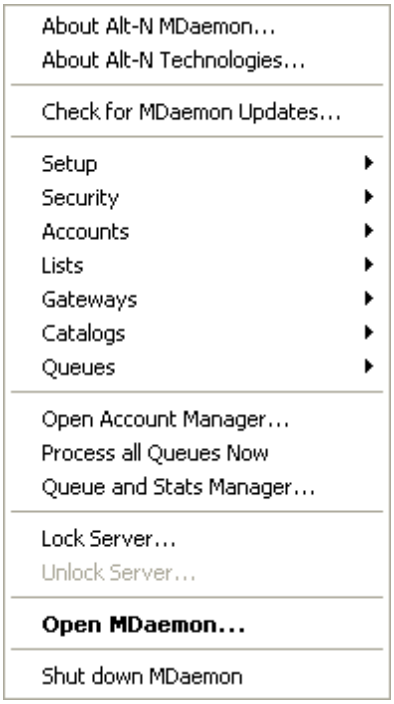
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Icon Blinking	A newer version of MDaemon is available.

There is additional information about the server available through the icon's tool tip. Pause the mouse pointer over it and the tool tip will appear, displaying the number of currently queued messages and active session.



Shortcut Menu



Right click on MDaemon's tray icon to open the shortcut menu. This menu gives you quick access to virtually all of MDaemon's menus without having to open the main user interface.

Click the "About Alt-N..." options in the top section of the shortcut menu to find out more about MDaemon or Alt-N Technologies.

In the next section, click "Check for MDaemon Updates..." to see if there is a newer version of MDaemon available for download.

In the third section you can access the following MDaemon menus: Setup, Security, Accounts, Lists, Gateways, Catalogs, and Queues. Each of these cascading menus is identical to the menu of the same name located on the menu bar of the main interface.

The fourth section has options to open the Account Manager and Queue and Statistics manager, and one that will cause all of MDaemon's mail queues to be processed.

Next, there are commands to lock and unlock MDaemon's interface (See "Locking/Unlocking MDaemon's Main Interface" below) followed by the "Open MDaemon..." menu selection, used for opening/restoring MDaemon's interface when it is minimized to the system tray.

The last option is "Shut down MDaemon," which is used to quit MDaemon or shut down its system service (the service settings are not changed—the MDaemon service is merely

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

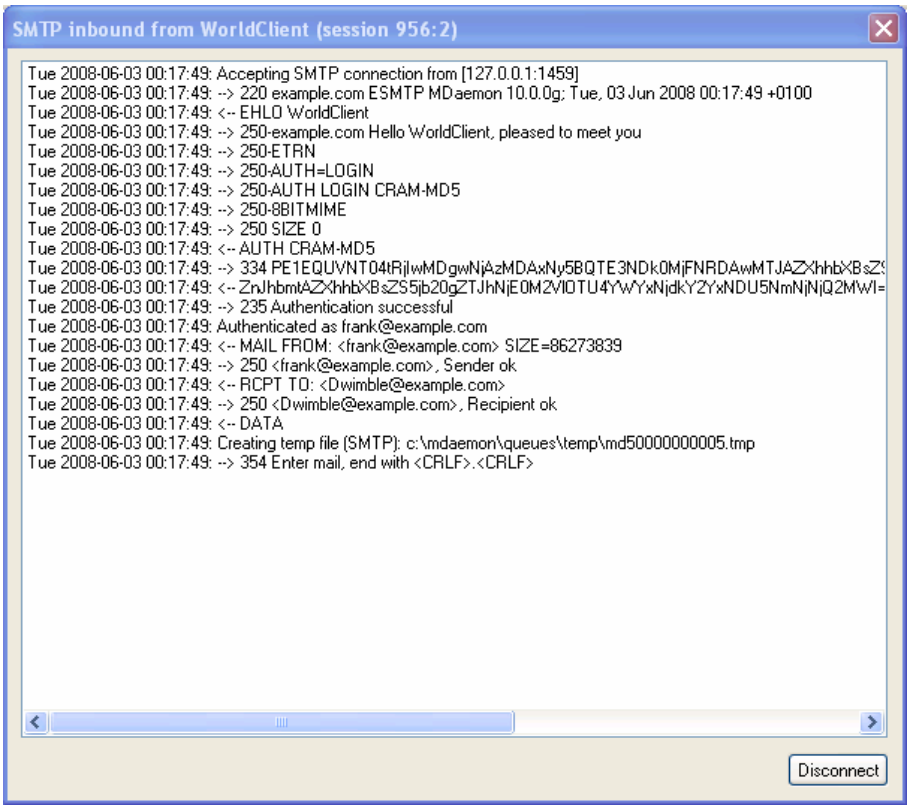
stopped).

Locking/Unlocking MDaemon's Main Interface

To lock the user interface, minimize MDaemon, click the "Lock server..." menu item and then enter a password into the box that opens. After confirming the password by entering it a second time, MDaemon's user interface will be locked. It cannot be opened or viewed, but MDaemon will continue to function normally. You will, however, still be able to use the "Process all queues now..." shortcut option to process the mail queues manually. To unlock MDaemon, open the "Unlock MDaemon" dialog by double-clicking the tray icon, or by right-clicking the icon and then choosing "Unlock Server..." Then, enter the password that you created when you locked it.

2.5 Session Window

When you double-click an active session on one of the Session tabs[41] of the main GUI, this will open the session window corresponding to that entry. The session window will display the SMTP transcript of that session as it progresses. You can click Disconnect on this window if you wish to interrupt and disconnect that session in progress.



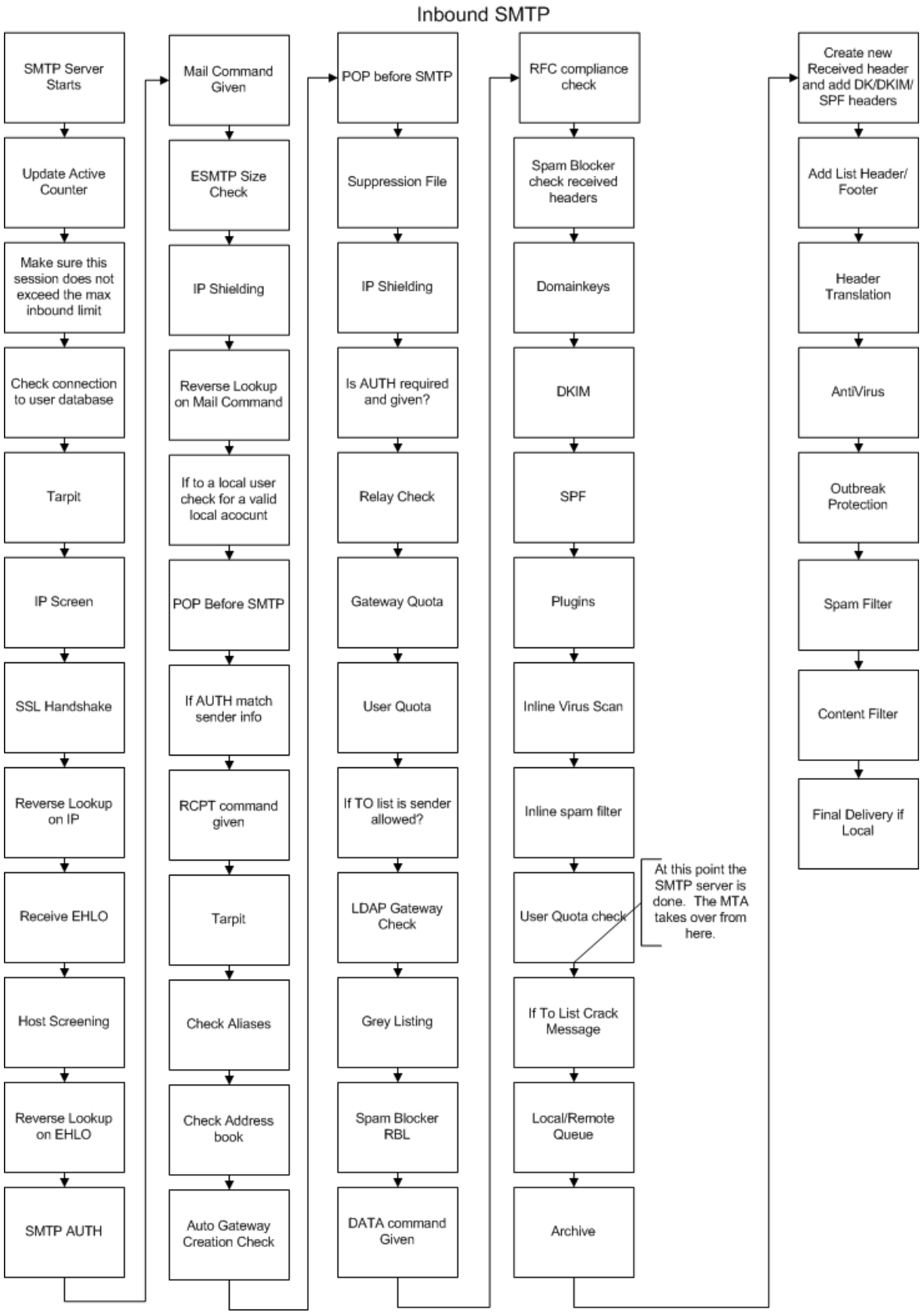
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

2.6 MDaemon's SMTP Work Flow

When an incoming SMTP connection is made, MDaemon goes through a complex series of processing steps to determine whether to accept the message for delivery, and what to do with it once it is accepted. The following chart is a graphical representation of this work flow for inbound SMTP messages.

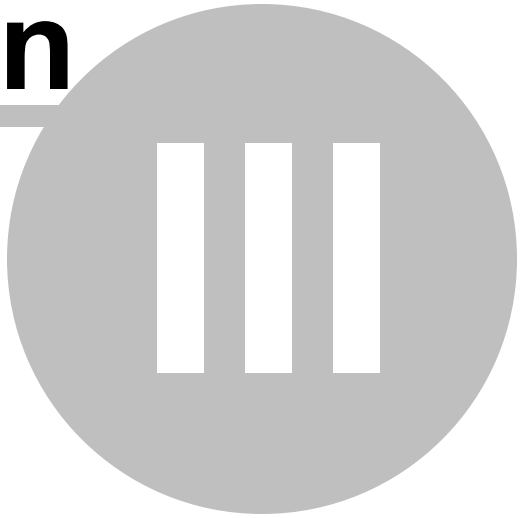
The extent to which these steps are executed is dependent upon your particular configuration. One or more steps might be skipped if a given feature is disabled in your configuration.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Section

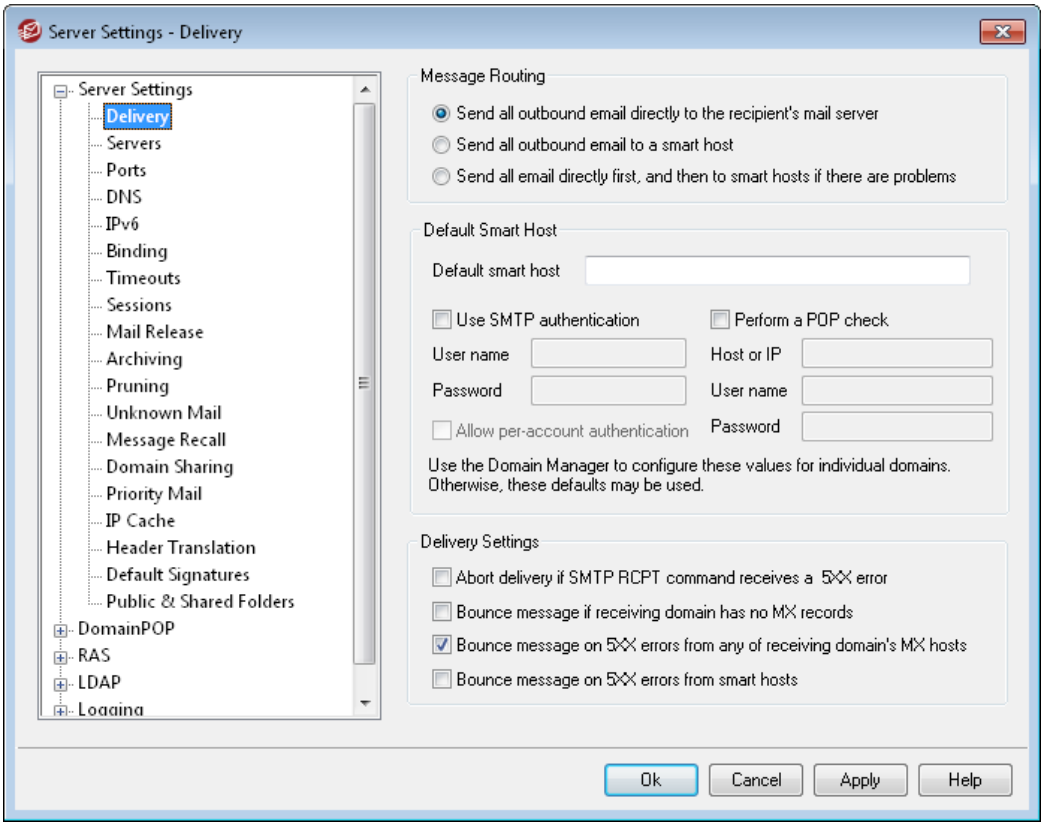


3 Setup Menu

3.1 Server Settings

3.1.1 Server Settings

3.1.1.1 Delivery



Message Routing

Send all outbound email directly to the recipient's mail server
When this option is chosen, MDaemon will attempt to deliver mail directly instead of passing it to another host. MDaemon will place undeliverable messages into its retry system and continue to attempt to deliver them according to the parameters and time intervals that you set on the Retry Queue 654 screen of the Mail Queues dialog.

Send all outbound email to a smart host
Select this option if you want outbound email, regardless of its destination domain, to be spooled to another host or server for routed delivery. If selected, outbound email will be sent to the *Default Smart Host* specified below. Typically, this feature is useful during high volume periods when direct message delivery would result in an excessive taxation of server resources. If a message cannot be delivered to the designated server then it will be moved into the retry system and MDaemon will continue to attempt to deliver it according to the parameters and time intervals that you set on the Retry Queue 654 screen of the Mail Queues dialog.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Send all email directly first, and then to smart hosts if there are problems
This option is a combination of the previous two delivery options. First MDaemon will attempt to deliver outbound email directly to the server, but if it is unable to deliver it, it will instead send the email to the *Default Smart Host specified below*. Undeliverable mail is email destined for hosts that could not be resolved to an actual IP address (such as an unregistered gateway to a remote network) or email destined for a host that was resolved properly but could not be connected to directly or is refusing direct connections. Rather than return such mail to its sender, this option causes MDaemon to pass the message off to a more powerful MTA. Sometimes the mail system run by your ISP may have routed methods of mail delivery to which your local server may not have direct access. If, however, a message cannot be delivered to the designated smart host then it will be moved to into the retry system and MDaemon will continue to attempt to deliver it according to the parameters and time intervals that you set on the Retry Queue 654 screen of the Mail Queues dialog. At each subsequent delivery attempt, MDaemon will again first try to deliver the message directly to its recipient and then to the designated smart host.

Default Smart Host

Default smart host
Specify your ISP or mail host's name or IP address here. This is generally the SMTP server on your ISP.

Do not enter MDaemon's Default Domain or IP addresses into this text box. This entry should be an ISP or other mail server that can relay mail for you.

Use SMTP authentication
Click this check box and enter your login credentials below if the *Default Smart Host* requires authentication. These login credentials will be used for all outbound SMTP messages sent to the smart host. If, however, you choose to use the *Allow per-account authentication* option below, then MDaemon will authenticate to the host separately for each message, using the sending account's *Smart Host Access* credentials designated on the Mail Services 525 screen of the Account Editor.

User name
Enter your user name or login here.

Password
Use this option to specify your smart host login password.

Perform a POP check first
If your smart host requires a POP3 check before it will accept messages from you, click this check box and enter your required credentials below.

Host or IP
Enter the host or IP address to which you wish to connect.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

User name
This is the POP account's login or account name.

Password
This is the POP account's password.

Allow per-account authentication
Click this checkbox if you wish to use per-account authentication for outbound SMTP messages sent to the *Default Smart Host* specified above. Instead of using the *User name* and *Password* credentials provided here, each account's *Smart Host Access* credentials, designated on the Mail Services 525 screen, will be used instead. If no smart host credentials have been designated for a given account, the above credentials will be used instead.

If you wish to configure *per-account authentication* to use each account's *Email password* instead of its optional *Smart host password*, then you can do so by editing the following key in the `MDaemon.ini` file:

```
[AUTH]
ISPAUTHUsePasswords=Yes (default No)
```

Enabling the `ISPAUTHUsePasswords=Yes` option will over time effectively communicate all your accounts' local mail passwords to your smart host. This could pose a risk to mail security, since it is providing sensitive information to another server. You should not use this option unless you are using a smart host that you absolutely trust and you believe it is necessary to do so. Further, you should note that if you use this option and give your users permission to change their *Email password* via WorldClient or some other means, then changing the *Email password* will also effectively change the *Smart host password*. This could cause smart host authentication to fail for an account when its *Email password* is changed locally but the corresponding *Smart host password* isn't changed at your smart host.

Abort delivery if SMTP RCPT command receives a 5xx error
Enable this option if you wish MDaemon to abort its attempt to deliver a message when it receives a 5xx fatal error in response to the SMTP RCPT command. This option is disabled by default.

Bounce message if receiving domain has no MX records
Ordinarily when MDaemon checks the receiving domain's DNS records, it will look for MX records and then for an A record when no MX records are found. If neither are found then it will bounce the message back to the sender as undeliverable. Click this option if you want MDaemon to immediately bounce the message when no MX record is found, instead of allowing it to then look for an A record also. This option is Disabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

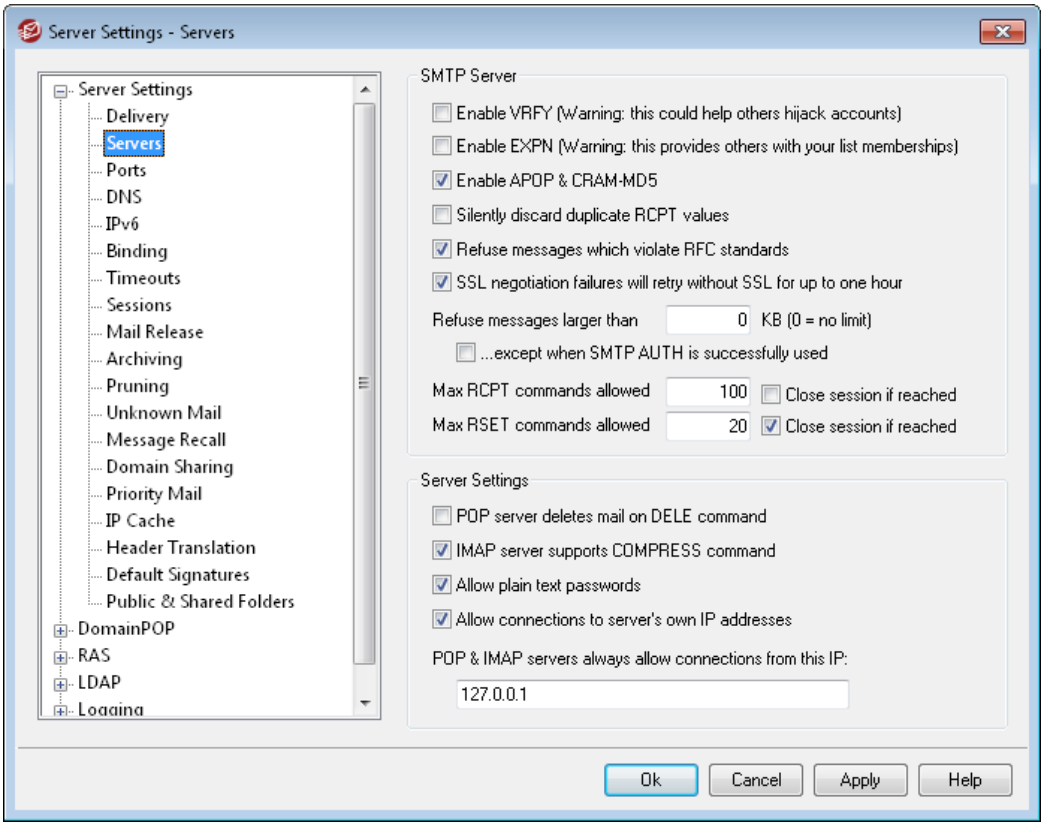
Bounce message on first 5XX error from any of receiving domain's MX hosts
When this checkbox is enabled, MDaemon will return/bounce the message when it receives a 5xx fatal error response from an MX host. Consequently, it won't continue trying to deliver the message to any subsequent MX hosts that may be designated for the recipient's domain. If this option is disabled, MDaemon won't bounce the message as long as at least one of the MX hosts returns a 4xx non-fatal error response. This option is enabled by default.

Bounce message on 5xx errors from smart hosts
Use this option if you wish to return/bounce a message when it receives a 5xx fatal error response from your smart hosts.

See:

Retry Queue 654
Mail Services 525

3.1.1.2 Servers



SMTP Server

Enable VRFY
Click this switch if you wish to respond to SMTP VRFY commands. This command is

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

sometimes used by servers that use an SMTP call forward or call back feature to attempt to confirm the validity of email addresses on your server. This is disabled by default.

Enable EXPN
Click this checkbox if you want MDaemon to honor EXPN commands.

Enable APOP & CRAM-MD5
By default MDaemon's servers (POP, IMAP, and so on) honor the APOP and CRAM-MD5 methods of authentication. These methods provide extra security by making it possible for users to be authenticated without sending clear text passwords. Clear this checkbox if you do not wish to allow APOP or CRAM-MD5.

Silently discard duplicate RCPT values
Enable this option if you want the SMTP server to ignore duplicate recipients in the same SMTP session. MDaemon will accept and then discard the duplicate recipients. This option is disabled by default.

Refuse messages which violate RFC standards
Enable this option if you wish to reject messages during the SMTP process that are not compliant to RFC internet standards. To pass the compliance test the message must:

1. Be greater than 32 bytes in size (the minimum size necessary to include all required parts).
2. Have either a FROM: or a SENDER: header.
3. Have no more than one FROM: header.
4. Have no more than one SUBJECT: header, though no subject header is required.

Messages using authenticated sessions or from trusted domains or IP addresses are exempt from this requirement.

SSL negotiation failures will retry without SSL for up to one hour
This option allows you to temporarily white list host IPs that encounter an SSL error during an outbound SMTP session. The white list is reset every hour.

Refuse messages larger than [xx] KB (0=no limit)
Setting a value here will prevent MDaemon from accepting or processing mail that exceeds a certain fixed size. When this option is enabled MDaemon will attempt to use the ESMTP SIZE command specified in RFC-1870. If the sending agent supports this SMTP extension then MDaemon will determine the message size prior to its actual delivery and will refuse the message immediately. If the sending agent does not support this SMTP extension then MDaemon will have to begin acceptance of the message, track its size periodically during transfer, and finally refuse to deliver the message once the transaction has completed. Use "0" in this option if you do not wish to set a size limit. If you wish to exempt authenticated sessions from SIZE checks, use the "*...except when SMTP AUTH is successfully used*" option below.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...except when SMTP AUTH is successfully used
Check this box if you wish to exempt messages from the message size limitation when the SMTP session is authenticated.

Max RCPT commands allowed
Use this option if you wish to limit the number of RCPT commands that can be sent per message. Use "0" if you do not wish to set a limit.

Close session if reached
Check this box if you wish to close the session immediately if the maximum allowed number of RCPT commands is reached.

Max RSET commands allowed
Use this option if you wish to set a maximum number of RSET commands allowed in an SMTP session (default is 20). Use "0" if you do not wish to set a limit.

Close session if reached
Check this box if you wish to close the session immediately if the maximum allowed number of RSET commands is reached.

Server Settings

POP server deletes mail on DELE command
Click this option if you wish MDaemon to delete messages immediately when they are retrieved and the DELE command is received, even if the POP session does not complete properly.

IMAP server supports COMPRESS command
Click this box if you wish to support the IMAP COMPRESS extension (RFC 4978), which compresses all data sent to and from the client. COMPRESS will increase CPU and memory usage per IMAP session.

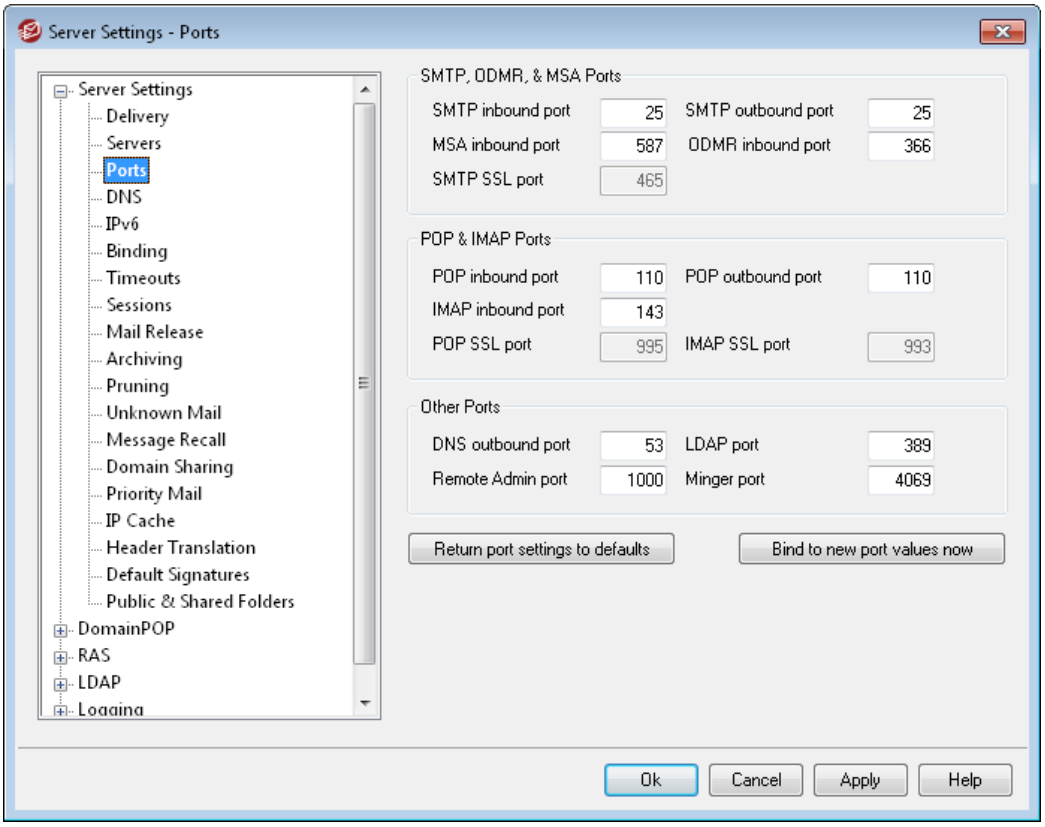
Allow plain text passwords
This option governs whether or not MDaemon will accept passwords sent in plain text to the SMTP, IMAP, or POP3 servers. If disabled, the `POP3 USER`, `POP3 PASS`, `IMAP LOGIN`, `IMAP AUTH LOGIN`, and `SMTP AUTH LOGIN` commands will return an error unless the connection is using SSL.

Allow connections to server's own IP addresses
When this option is enabled, MDaemon can connect to itself.

POP & IMAP servers always allow connections from this IP
The POP and IMAP servers will always accept connections from the IP Address entered into this field regardless of screening and shielding settings.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.3 Ports



SMTP, ODMR, & MSA Ports (some features require MDaemon PRO)

SMTP inbound port
MDaemon will monitor this TCP port for incoming connections from SMTP clients. This is the main SMTP port, which in most cases should be left at the default setting of port 25.

SMTP outbound port
This port will be used when mail is sent to other SMTP servers.

MSA inbound port
This is a Message Submission Agent (MSA) port that can be used by your users as an alternative to the *SMTP inbound port* specified above. Transmission on this port requires AUTH, therefore users sending on that port must configure their mail clients appropriately to ensure that their connections are authenticated. Further, because some ISPs block port 25, your remote users might be able to circumvent that restriction by using the MSA port instead. If you do not wish to designate an MSA port then set the value to "0" to disable it.

Connections to the MSA port are exempt from PTR and reverse lookups, Host and IP screening, the IP Shield, and Tarpitting. MSA port connections continue to utilize dictionary attack

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

connection limiting.

ODMR inbound port
MDaemon will monitor this port for incoming On-Demand Mail Relay (ODMR) connections, such as `ATRN` from Gateway Domains.

SMTP SSL port
This is the port dedicated to SMTP mail sessions using a Secure Sockets Layer (SSL) connection. See SSL & Certificates 487 for more information.

POP & IMAP Ports (some features require MDaemon PRO)

POP inbound port
MDaemon will monitor this port for incoming connections from remote POP clients.

POP outbound port
This port will be used when MDaemon retrieves mail from POP servers.

IMAP inbound port
MDaemon will monitor this port for incoming IMAP requests.

POP SSL port
This is the port dedicated to POP mail clients using a Secure Sockets Layer (SSL) connection. See SSL & Certificates 487 for more information.

IMAP SSL port
This is the port dedicated to IMAP mail clients using a Secure Sockets Layer (SSL) connection. See SSL & Certificates 487 for more information.

Other Ports

DNS outbound port
Enter the Port you want MDaemon to use for sending and receiving datagrams to the DNS server.

LDAP port
MDaemon will post database and address book information to your LDAP server on this port.

See: LDAP Address Book Support 105

Remote Admin port
This is the port that MDaemon will monitor for Remote Administration 251 connections.

Minger port
This is the port that the Minger 640 server will monitor for connections.

Return port settings to defaults
This button returns all the port settings to their standard values.

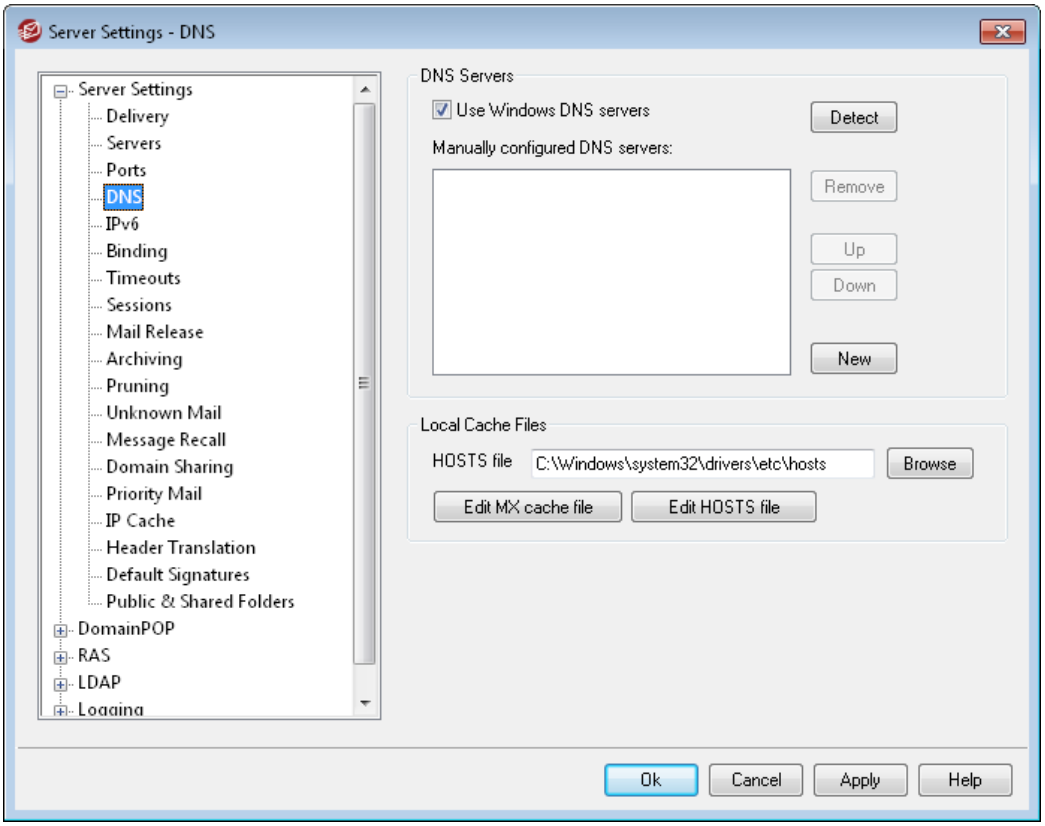
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Bind to new port values now
When you alter the values of any of the port settings you will need to press this button to have your changes take immediate effect. Otherwise, your changes will not be put into place until the next time the server is started.

The preceding port settings are critical for proper server operation and should not be altered unless you are certain that you must do so. Being able to configure the ports that MDaemon uses will allow you to configure the server to operate with proxy systems or other software services that require certain port numbers.

An IP address (a machine) has only one of each available port. If one program attempts to gain access to a port that is already in use by another program, an error message will inform the user that the requested address (IP:PORT) is already in use.

3.1.1.4 DNS



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

DNS Servers

Use Windows DNS servers
When this option is selected, MDaemon will use all DNS servers found within your Windows TCP/IP configuration. MDaemon will try each DNS server once per lookup operation and in sequence until it exhausts the complete list of DNS servers or finds the first one that works. If you include additional DNS servers in the *Manually configured DNS Servers* option below, MDaemon will try those servers as well. Finally, at startup the System log will display each DNS server and indicate its source (i.e. manually configured or taken from Windows).

Manually configured DNS servers
MDaemon will use all DNS servers specified here when performing DNS lookups. MDaemon will try each server once per lookup operation and in sequence until it exhausts the complete list of DNS servers or finds the first one that works. If you enable the *Use Windows DNS servers* option above, MDaemon will also query all DNS servers found within your Windows TCP/IP configuration. Finally, at startup the System log will display each DNS server and indicate its source (i.e. manually configured or taken from Windows).

Local Cache Files

Hosts file...
Before querying the DNS servers, MDaemon will first attempt to resolve an address by processing the Windows HOSTS file. If this file contains the IP address of the domain in question, MDaemon will not need to query the DNS server.

You must enter the complete path and filename rather than just the filename. MDaemon will attempt to use the following value as the default location of this file:

[drive]:\windows\system32\drivers\etc\hosts

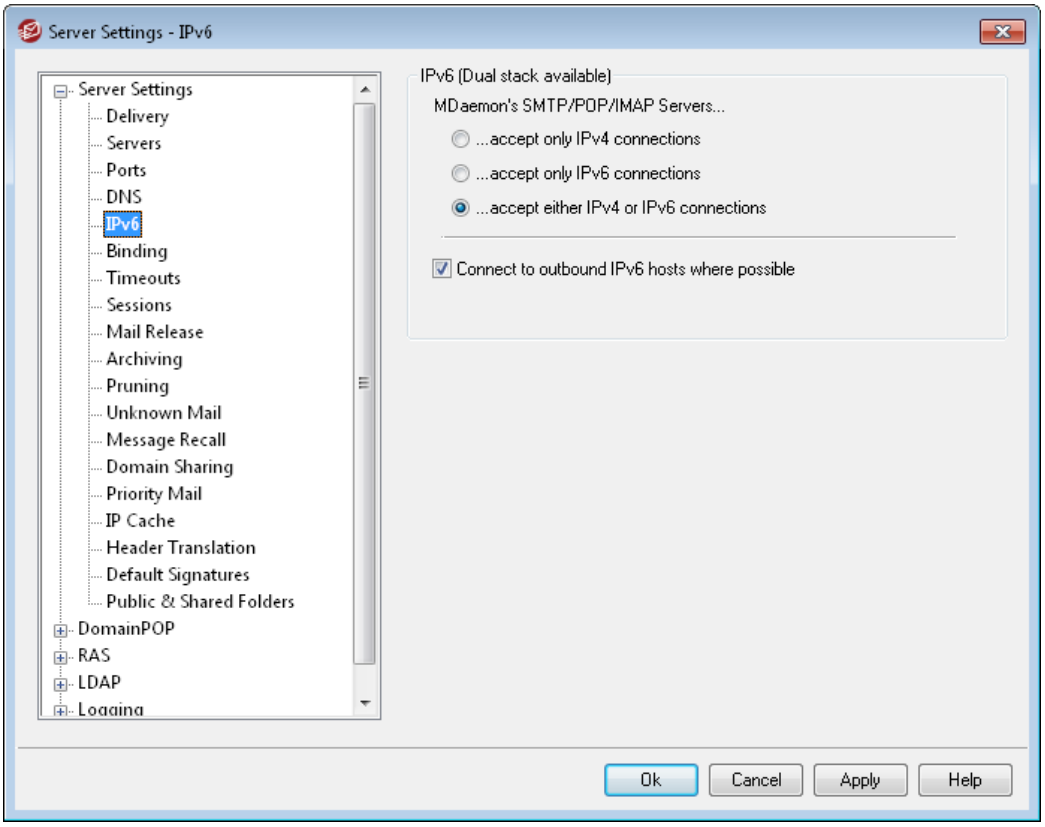
The HOSTS file is a Windows file that contains the A-record or primary IP address for domain names. MDaemon also allows you to specify MX-record IP addresses within a file called MXCACHE.DAT. This file can be found within the MDaemon\APP \ subdirectory. Load the MXCACHE.DAT file into a text editor and read the comments at the top of the file for more information.

Edit MX cache file
Click this button to view or edit the MXCACHE.DAT file with a text editor.

Edit hosts file
Click this button to view or edit the HOSTS file with a text editor.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.5 IPv6



By default MDaemon detects the level of IPv6 capability that your OS supports and dual-stacks where possible. Otherwise, MDaemon monitor both IPv4 and IPv6 independently.

IPv6 (Dual stack available)

MDaemon's SMTP/POP3/IMAP Servers...

...accept only IPv4 connections
Choose this option if you only wish to accept IPv4 connections.

...accept only IPv6 connections
Choose this option if you only wish to accept IPv6 connections.

...accept either IPv4 or IPv6 connections
Choose this option if you wish to accept both IPv4 and IPv6 connections. This is the default setting, and MDaemon will give precedence to IPv6 connections over IPv4 whenever possible.

Connect to outbound IPv6 hosts where possible
By default, MDaemon will connect to outbound IPv6 hosts whenever possible.

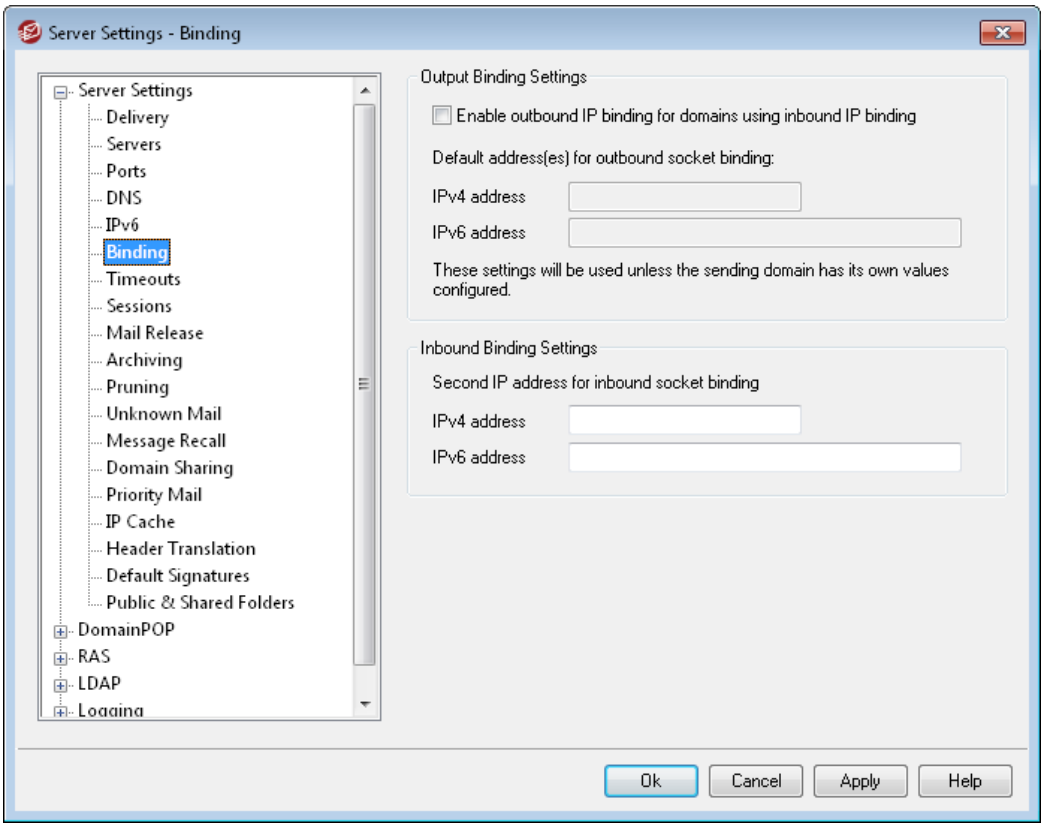
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

When MDaemon connects to an IPv6 host it must use an IPv6 local address of its own. The IPv6 address is designated on the Domain Manager » Host Name & IP 124 screen. If necessary, an address for outbound socket binding can be specified on the Binding 61 screen.

See:

Binding 61
Domain Manager » Host Name & IP 124

3.1.1.6 Binding



Enable outbound IP binding for domains using inbound IP binding
Click this option to cause domains that are using the *This domain recognizes only connections made to these IPs* 124 option to also restrict outbound sockets. The IP addresses that will be used are the same ones that are associated with the handling of inbound mail, unless different ones are specified below.

Default address(es) for outbound socket binding: IPv4/IPv6 address
These are the IP addresses that will be used for outbound socket binding for domains that are not already bound to specific IP addresses on the Domain Manager's Host Name & IP 124 screen.

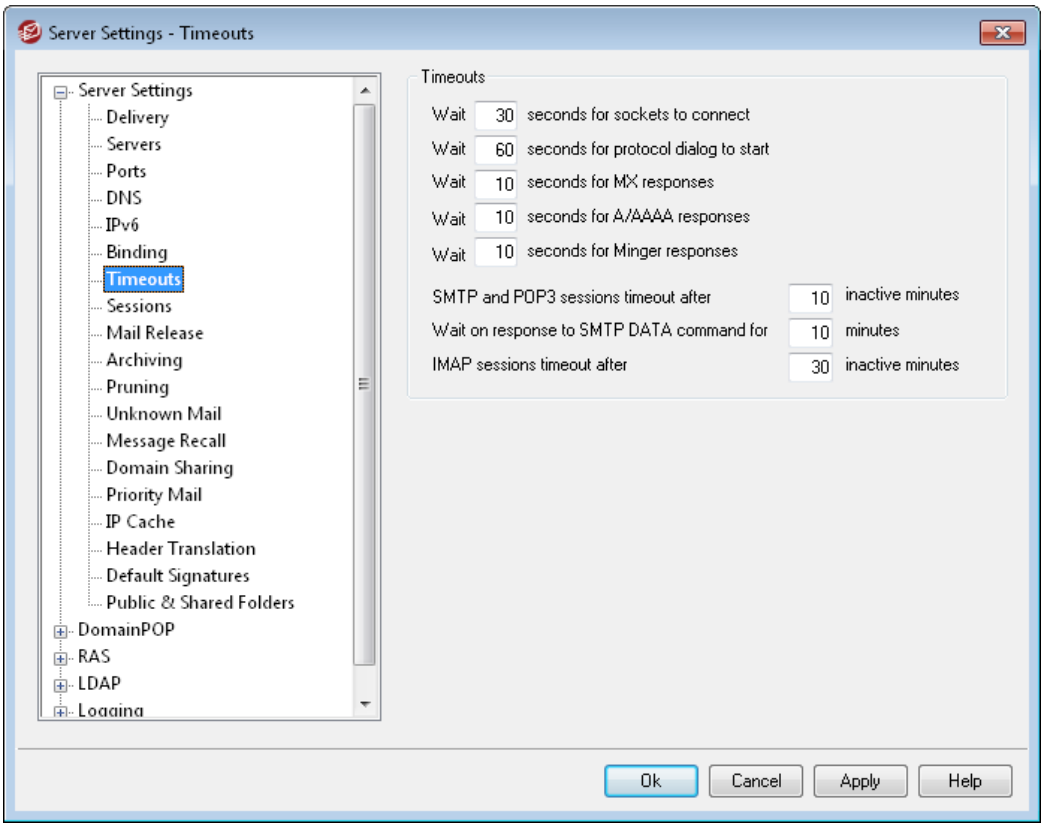
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Second IP address for inbound socket binding: IPv4/IPv6 address
Use this option if you wish to designate a second set of IP addresses for inbound socket binding 124.

See:

Domain Manager » Host Name & IP 124
IPv6 60

3.1.1.7 Timeouts



Timeouts

Wait xx seconds for sockets to connect
After initiating a connection request MDaemon will wait this many seconds for the remote system to accept the connection. If the remote system does not respond within this time frame, MDaemon will send the message to a specified *smart host* or place it into the retry system, depending upon which option you have chosen on the Delivery 50 screen of the Server Settings dialog.

Wait xx seconds for protocol dialog to start
Once a connection has been established with a remote host, this is the number of seconds that MDaemon will wait for the remote host to begin the SMTP or POP3 protocol dialog. If the remote host does not begin the protocol session within this time frame, MDaemon will send the message to a specified *smart host* or place it

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

into the retry system, depending upon which option you have chosen on the Delivery 50 screen of the Server Settings dialog.

Wait XX seconds for MX responses
While using DNS services to resolve 'MX' hosts for remote domains, MDaemon will wait for responses to its 'MX' queries for this number of seconds. If the DNS server does not respond within this time frame MDaemon will attempt to deliver the message to the IP address specified in the remote host's 'A' DNS record. If that attempt fails, MDaemon will send the message to a specified *smart host* or place it into the retry system, depending upon which option you have chosen on the Delivery 50 screen of the Server Settings dialog.

Wait XX seconds for A/AAAA responses
This timer governs how long MDaemon will wait while attempting to resolve a remote host's IP address. If the attempt fails, MDaemon will send the message to a specified *smart host* or place it into the retry system, depending upon which option you have chosen on the Delivery 50 screen of the Server Settings dialog.

Wait XX seconds for Minger responses
This the the number of seconds that MDaemon will wait for a response from a Minger 640 server.

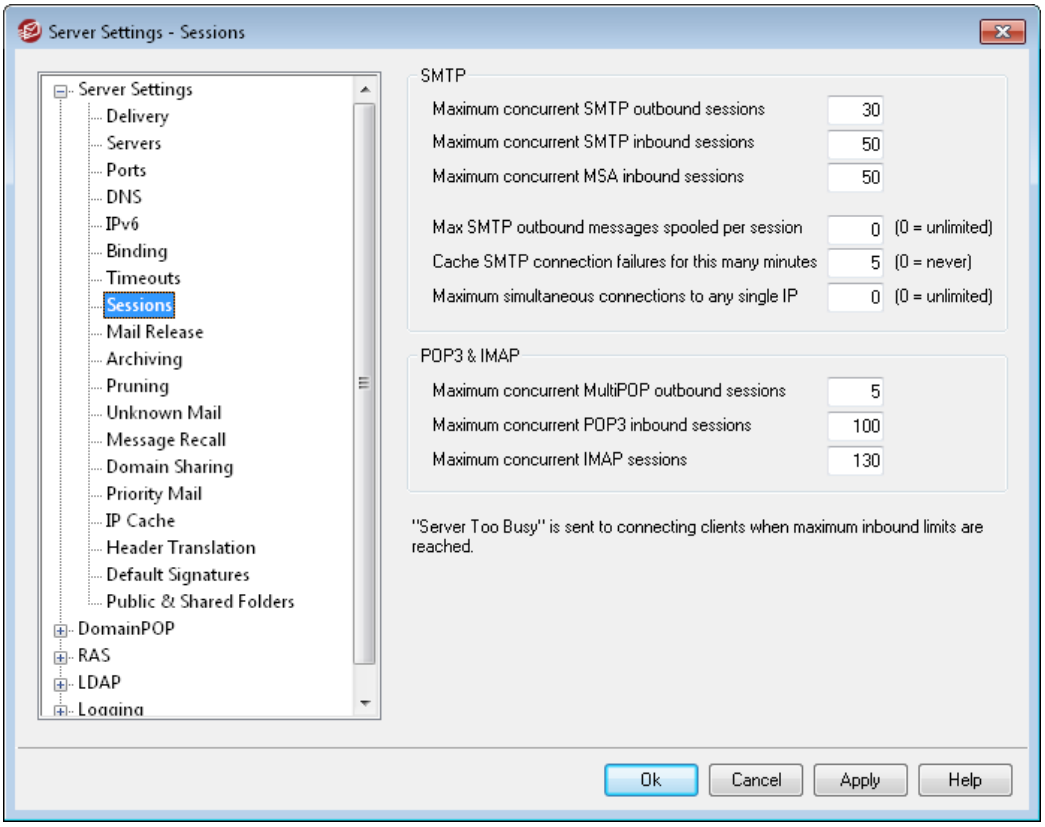
SMTP and POP3 sessions timeout after XX inactive minutes
If a successfully connected and operating session remains inactive (no i/o) for this length of time, MDaemon will abort the transaction. MDaemon will try again at the next scheduled processing interval.

Wait on response to SMTP DATA command for XX minutes
This option governs how long MDaemon will wait for the "`250 Ok`" response after sending the `DATA` command during the SMTP process. Since some receiving servers perform lengthy anti-spam, anti-virus, or other necessary operations at that time, this option can be used to give them time to complete those tasks. The default is 10 minutes.

IMAP sessions timeout after xx inactive minutes
If an IMAP session has no activity for this number of minutes, MDaemon will close the session.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.8 Sessions



SMTP

Maximum concurrent SMTP outbound sessions
The value entered here represents the maximum possible outbound SMTP sessions that will be created when it is time to send outbound mail. Each session will send outbound messages until either the queue is empty or the *Maximum SMTP outbound messages spooled per session* setting has been reached. For example, if the outbound mail queue has twenty messages waiting when it is time to send mail and the value of this setting is five, then five sessions will be simultaneously created and each will consecutively deliver four messages.

This option is set to 30 by default, but you may wish to experiment with the number of sessions in order to find the setting that will yield the best performance for your bandwidth. It is possible to specify so many sessions that your bandwidth will be overloaded or your Windows machine will run out of resources and you will lose delivery efficiency. Remember, each SMTP session created by MDaemon will deliver messages consecutively and therefore four sessions delivering two messages each might perform better and faster than eight threads delivering only one message each. A good place to start would be five to ten threads when using a 56k modem and twenty to thirty for broadband

Maximum concurrent SMTP inbound sessions
This value controls the number of concurrent inbound SMTP sessions that the server will accept before it begins responding with a "Server Too Busy" message. The

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

default value is 50.

Maximum concurrent MSA inbound sessions
Use this option to designate the maximum number of concurrent mail submission agent (MSA) inbound sessions allowed.

Maximum SMTP outbound messages spooled per session
This setting places a limit on the number of individual messages that each session will send before it stops delivering mail and frees itself from memory. Ordinarily, you should leave this control set to zero, which will cause each session to continue delivering messages until the queue is empty.

Cache SMTP connection failures for this many minutes (0 = never)
When an SMTP connection to a given host fails, MDaemon will cease trying to connect to that host for the number of minutes specified in this option. This can prevent MDaemon from needlessly attempting to connect to a problem host over and over again when, for example, it has multiple messages designated for that host and yet discovers that it is down when making the first delivery attempt. The default setting is "5" minutes. Use "0" if you do not wish to cache SMTP failures.

Maximum simultaneous connections to any single IP (0 = unlimited)
Use this option to limit the number of simultaneous connections that will be allowed to a single IP address during mail delivery. Use "0" if you do not wish to limit simultaneous connections.

This option is useful to prevent making too many connections at once to various IP addresses. During delivery, if a message would require a connection to an IP that would exceed this connection limit, then the connection is skipped and the next MX host (or smart host) is used. If no additional hosts are available the message is queued for the next delivery cycle. By default, this option is disabled, which preserves existing behavior. Also by default, connections to trusted IP addresses are exempt from this feature. However, if you'd like to enforce it for trusted IPs you can set the following in the `MDaemon.ini` file:

```
[Sessions]
TrustedIPsUseConnectionLimit=Yes (default No)
```

Also by default, connections to IP addresses reserved for intranet use are exempt from this feature. These are `127.0.0.*`, `192.168.*.*`, `10.*.*.*`, and `172.16.0.0/12`. However, if you'd like to enforce it for reserved IP addresses you can set the following in the `MDaemon.ini` file:

```
[Sessions]
ReservedIPsUseConnectionLimit=Yes (default No)
```

POP3 & IMAP

Maximum concurrent MultiPOP outbound sessions
The value entered here represents the maximum possible outbound POP sessions that will be created when it is time to collect MultiPOP mail. Each session will collect this type of mail until all MultiPOP servers have been processed, and all mail has been collected. For example, if there are fifteen MultiPOP sessions amongst all of

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

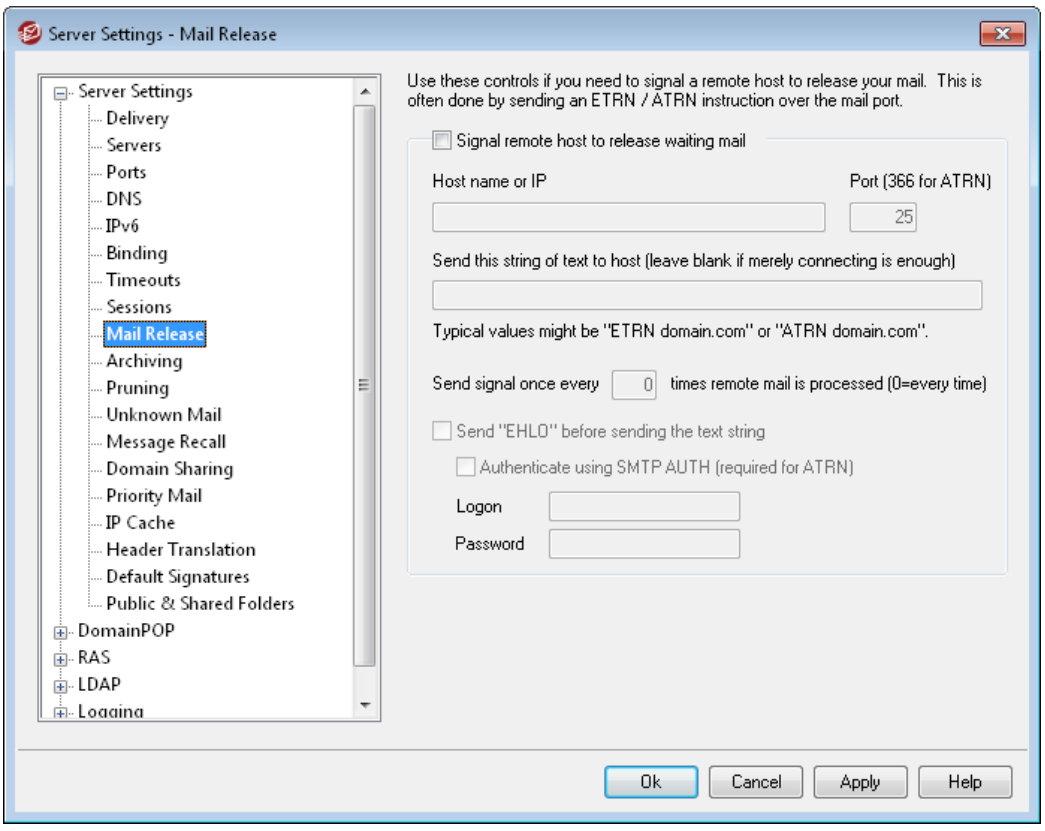
your users and the value of this setting is set to three, then each session will collect mail from five MultiPOP sources.

You should experiment with the number of sessions to determine what number will yield the best performance for your bandwidth. It is possible to specify so many sessions that your bandwidth will be overloaded, or your Windows machine will run out of resources and you will lose processing efficiency. Remember that each POP sessions created by MDaemon will collect mail until all sources have been exhausted. Therefore, four sessions collecting mail from twenty sources might perform better and faster than twenty sessions collecting from a single source.

Maximum concurrent POP3 inbound sessions
This value controls the maximum number of concurrent POP inbound mail sessions that the server will accept before it begins responding with a "Server Too Busy" message.

Maximum concurrent IMAP sessions
This value controls the maximum number of concurrent IMAP mail sessions that the server will accept before it begins responding with a "Server Too Busy" message.

3.1.1.9 Mail Release



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Signal remote host to release waiting mail

When it is time to process remote mail MDaemon can connect to any server on any port and send any string that you wish to send. This is useful when you need to signal a remote server to release your mail by sending some string to them. For example, ATRN, ETRN, or QSND. You can also use this feature when a FINGER or TELNET session is briefly required in order for your remote host or ISP to determine that you are online.

Host name or IP
This is the host that will be signaled to release your mail.

Port
Enter the port on which you wish to make the connection. The default is 25 (the SMTP port), which is appropriate for the ETRN or QSND signaling method. Port 366 is typically used for ATRN, and port 79 is used for FINGER.

Send this string of text to host (leave blank if merely connecting is enough)
This control is for specifying the text string that needs to be sent in order for your mail to be released. For example, the ETRN method requires the text "ETRN" followed by the domain name of the site being queued. Other methods require different text to be sent. Consult your ISP if you need more information on what to send to unlock your mail queue. If you have a choice of the method to use, we recommend using On-Demand Mail Relay (ODMR) 681 whenever possible. ODMR requires the ATRN command to be used in this option.

Send signal once every [xx] times remote mail is processed (0=every time)
By default the dequeue signal will be sent each time that remote mail is processed. Entering a number into this control will prevent the dequeue signal from being sent every time. It will be sent every x number of times as designated. For example, setting this value to "3" would cause the signal to be sent every third time that remote mail is processed.

Send "EHLO" before sending the text string
If you enable this checkbox then you should be connecting to an SMTP server to signal release of your mail. This switch causes an SMTP session to be initiated with the specified host and allows the session to progress just beyond the SMTP "EHLO" stage before sending the unlock string.

Authenticate before sending the text string (required for ATRN)
As a security measure, some hosts or servers require clients to authenticate using ESMTP AUTH before releasing waiting messages. If this is the case for your mail host, click this checkbox and enter the required authentication credentials below.

Authentication is required when using the ATRN command to dequeue your email.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Logon
Enter the AUTH logon parameter here that is required by your host.

Password
Enter the AUTH password here.

3.1.1.9.1 On-Demand Mail Relay (ODMR)

When you require a queue/dequeue method for hosting and releasing your email, we recommend using On-Demand Mail Relay (ODMR) whenever possible. This method is superior to ETRN and other methods in that in requires authentication before mail is released. Further, it utilizes an ESMTP command called `ATRN` that does not require the client to have a static IP address, because it immediately reverses the flow of data between the client and server, releasing the messages without having to make a new connection to do so (unlike ETRN).

MDaemon fully supports ODMR on the client side via using the `ATRN` command and authentication controls on the Mail Release 66 screen, and on the server side using the Domain Gateways features on the Dequeuing 175 screen of the Gateway Editor.

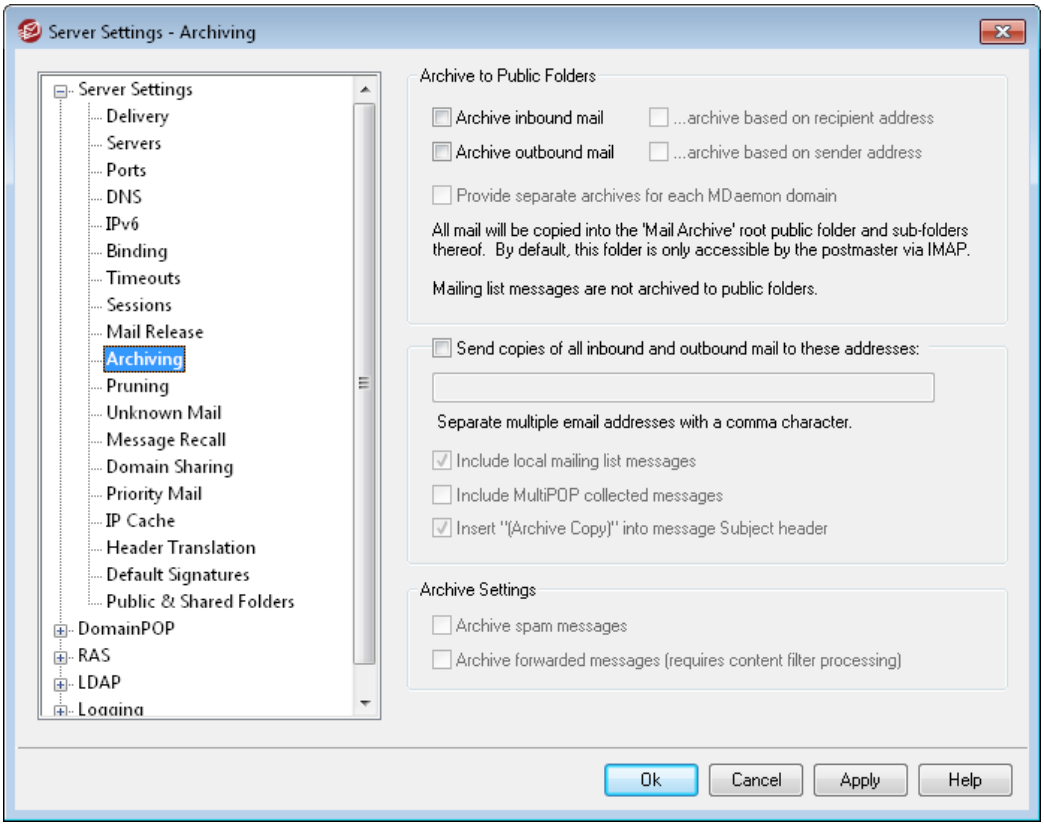
Some mail servers do not support ODMR, therefore you should check with your provider before attempting to use it.

See:

Gateway Editor » Dequeuing 175

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.10 Archiving



Archive to Public Folders

Archive inbound mail
Click this check box to save a copy of all inbound messages into the Mail Archive root public folder and its subfolders. By default, this folder is accessible only by the Postmaster via IMAP. If you want to alter the permissions or grant access to more users you can do so by using the Access Control List 220.

...archive based on recipient address
Click this option if you want the inbound mail archive to be categorized by the recipient's email address.

Archive outbound mail
Click this check box to save a copy of all outbound messages in the Mail Archive public folder. By default, this folder is only accessible only by the Postmaster via IMAP. If you want to alter the permissions or grant access to more users you can do so by using the Access Control List 220.

...archive based on sender address
Click this option if you want the outbound mail archive to be categorized by the sender's email address.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Provide separate archives for each MDaemon domain
Click this option if you want to maintain a separate archive for each domain.

Send copies of all inbound and outbound mail to these addresses

Enter one or more addresses to which you wish to send archival messages. Multiple addresses must be separated by a comma. You may specify local and remote addresses and address aliases.

Include local mailing list messages
When this option is enabled, archived mail will include your mailing list messages.

Include MultiPOP collected messages
Enable this option if you wish to archive messages collected through MDaemon's MultiPOP 544 feature.

Insert "(Archive Copy)" into message Subject header
When this option is enabled, "(Archive Copy)" will be inserted in the `Subject:` header of archived mail.

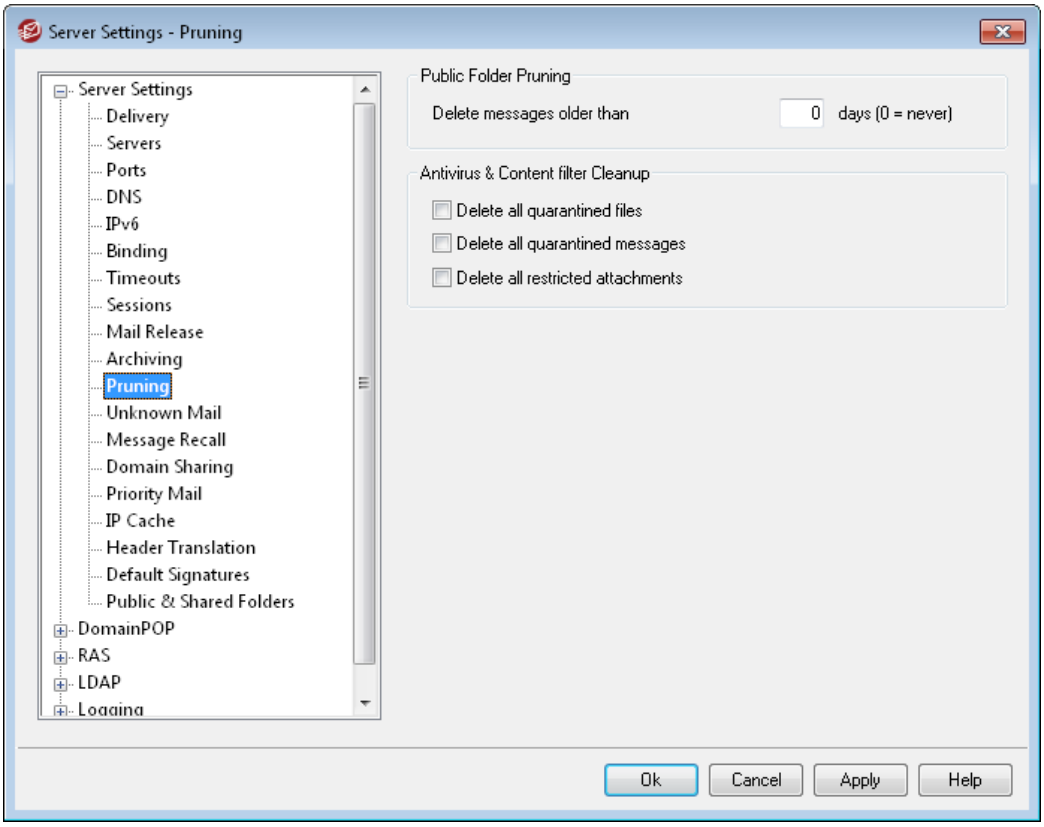
Archive Settings

Archives spam messages
Enable this option if you wish the archives to include messages that are marked as spam.

Archive forwarded messages (requires content filter processing)
Enable this option if you want the archives to include messages that are forwarded. By default these are not archived.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.11 Pruning



Public Folder Pruning

Delete messages older than XX days (0=never)
Specify a number of days in this option if you want old messages to be deleted from Public Folders 84.

Antivirus & Content Filter Cleanup

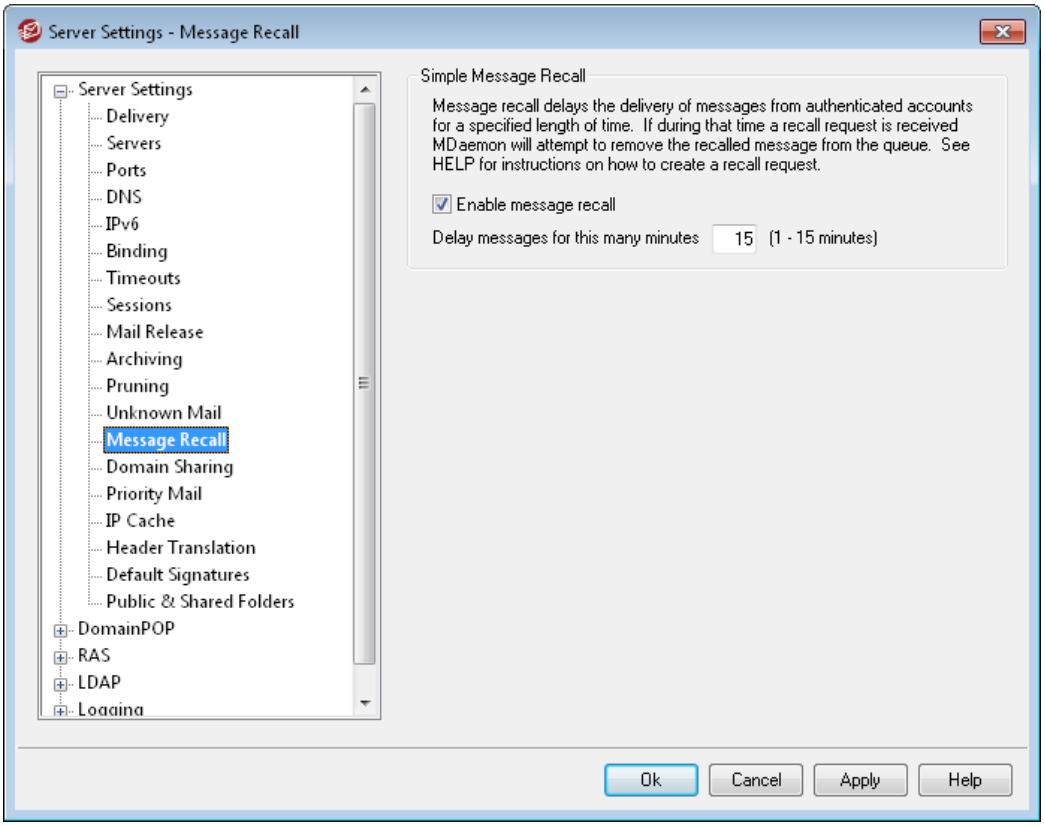
Delete all quarantined files
Click this option if you want all quarantined file attachments to be deleted each night.

Delete all quarantined messages
Click this option if you want all quarantined messages to be deleted each night.

Delete all restricted attachments
Click this option if you want all restricted attachments to be deleted each night.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.12 Message Recall



Simple Message Recall

MDaemon Pro has a simple message recall system that you can use to delay incoming messages sent by authenticated local users for 1 to 15 minutes. During that delay period the messages are simply left in the inbound mail queue. This provides a short period during which a user can attempt to stop a message from being delivered. Once the delay period expires the message is delivered normally.

To recall a message a user can simply log in to WorldClient and click the *Recall* button that will be displayed when viewing a recently sent message in the Sent Items folder. If clicked before the recall time limit expires, WorldClient will send a RECALL message to MDaemon. Alternatively, the user can go the the Sent Items folder in his mail client, locate the message he wishes to recall, and then "Forward as Attachment" the message to the `mdaemon@example.com` system account, using "`RECALL`" as the message's Subject. Another alternative is to view the message's headers, copy the "`Message-ID: <message-ID value>`" header, and create a new message with "`RECALL Message-ID: <message-ID value>`" in the subject (without the quotes). If both alternatives are used within the same recall message, only the message ID option will be used.

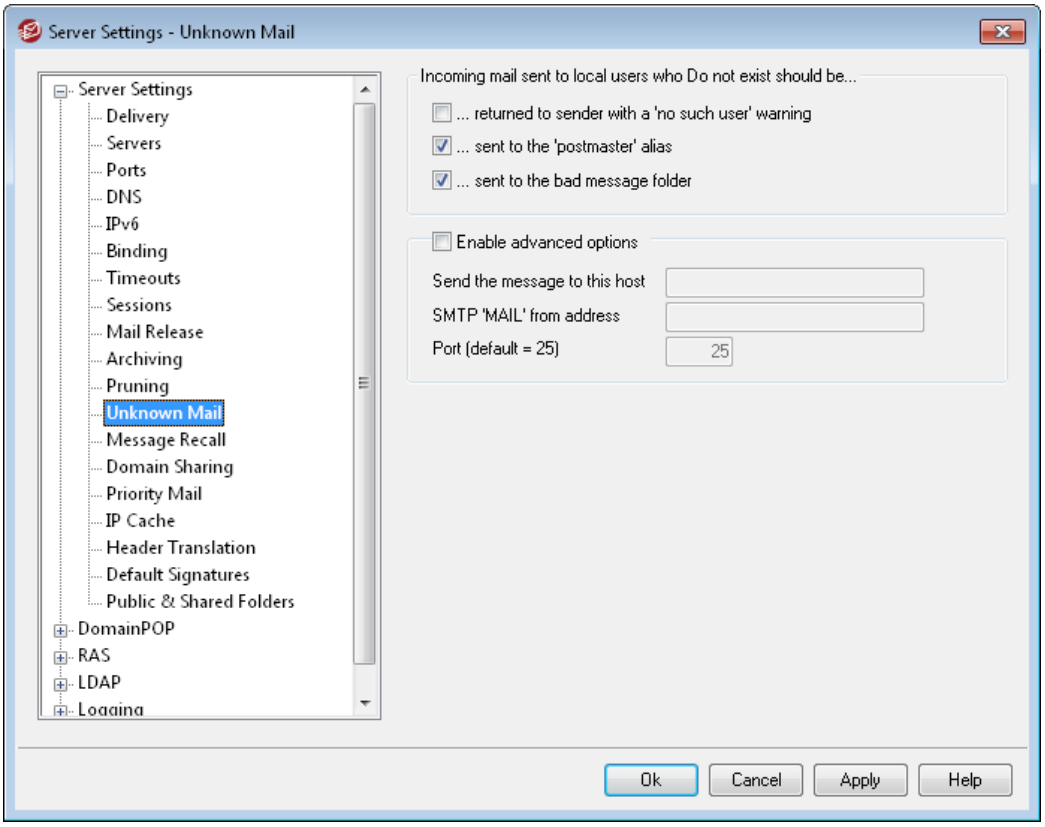
Regardless of the chosen recall method, MDaemon will send an email back to the user, saying whether or not the recall was successful. When a message is successfully recalled, MDaemon deletes the message from the inbound queue as if it had never been sent. All recall processing is logged to MDeamon's Routing log.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Enable message recall
Click this checkbox to activate the message recall system. The option is disabled by default.

Delay messages for this many minutes XX (1-15 minutes)
This is the number of minutes that MDaemon will hold incoming messages from authenticated local users. If a RECALL message is received during the delay period then MDaemon will delete the referenced message. This option can be set to 1-15 minutes. 1 minutes is the default setting.

3.1.1.13 Unknown Mail



Incoming mail sent to local users who do not exist should be...

...returned to sender with a 'no such user' warning
When this option is enabled, messages that arrive at the server destined for unknown yet supposedly local users will be returned to the message originator.

...sent to the 'Postmaster' alias
By default, messages that arrive at the server destined for unknown yet supposedly local users will be forwarded to whatever user has been aliased as the postmaster. Disable this option if you do not wish to send these messages to the Postmaster.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...sent to the bad message folder
By default, messages that arrive at the server destined for unknown yet supposedly local users will be routed to the bad message queue. Clear this checkbox if you do not wish to send these messages to the bad message queue.

Advanced Options

Enable advanced options
Click this checkbox to enable the following advanced mail routing properties.

Send the message to this host
If a mail host is specified here, messages addressed to unknown local users will be sent to it.

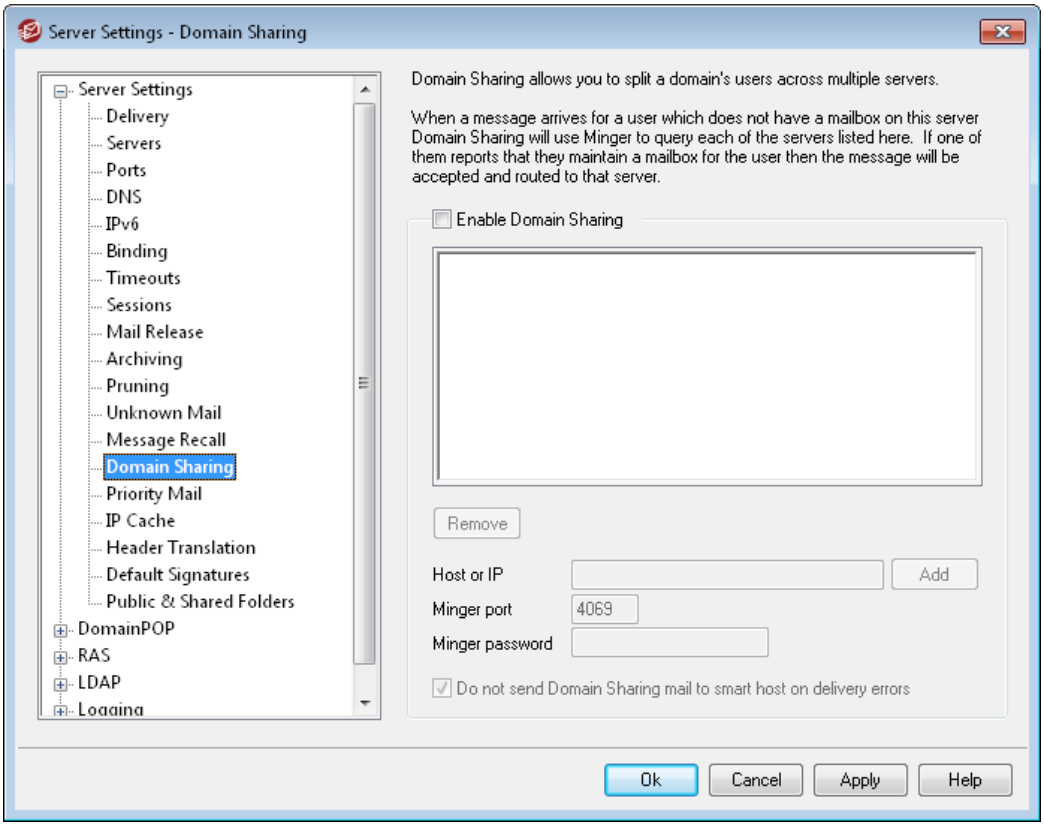
The following applies globally anywhere within MDaemon where you are allowed to specify a host to forward, copy, or send email to. If you enclose the host in brackets (e.g. `[example.com]`), MDaemon will skip MX record lookups when delivering to that host. For example, if this option contained "`example.com`" then MX lookups would be performed normally. If, however, that option contained "`[example.com]`" then only the A-record lookup would be performed.

SMTP 'MAIL' from address
This address will be used in the SMTP "`Mail From:`" statement used during the session handshaking with the accepting host. Normally the sender of the message is used in this portion of the SMTP envelope. If you require an empty command (`MAIL FROM <>`) then enter "`[trash]`" into this control.

Port (default = 25)
This is the TCP port that MDaemon use to send the message. The default value is port 25.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.14 Domain Sharing



Domain Sharing is a feature which allows you to split a domain's users across multiple servers. This makes it possible for you to have MDaemon servers running in different locations, all using the same domain names but with different user accounts. One portion of your domains' user accounts are hosted on one server while another portion of them are hosted on one or more other servers. The Domain Sharing dialog is used to specify where each of these other servers is located. Then, when an incoming message arrives for a local user who does not have a local mailbox, Domain Sharing will use Minger to query the other servers in order to discover whether or not that user has an account on one of them. If the address is found to be valid, MDaemon will accept the message and route it to the server where the account is located.

For example, you could have offices in multiple cities and choose to use Domain Sharing to allow every employee to have an email address ending with, "`@example.com`." Each office's MDaemon would host a portion of `example.com's` email, having accounts only for the local employees who work in that office. Then, every office would be configured to use Domain Sharing, so that everyone's messages would get routed to the correct office.

Because Domain Sharing uses Minger 640 to verify addresses, Minger must be enabled and properly configured on each server in order for queries to function. If, however, an error occurs during a Minger query, such as when one of the servers is temporarily unavailable, MDaemon will respond with a "451" temporary error code so that the sending server can try to deliver the message again later. Further, once an address has been verified, it will be cached for five days so that MDaemon can immediately accept future messages for that address and begin attempting to route those messages to the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

proper host.

Finally, to avoid potential problems that could occur if the same account were created on multiple servers, MDaemon will query all of the Domain Sharing servers before creating any new account.

There is an option called "*Minger verification lookups also trigger Domain Sharing lookups*," located on the Gateway Editor's Settings 179 screen. This option can be used to cause MDaemon to also query your Domain Sharing hosts whenever Minger Verification 170 is used by a Gateway.

Enable Domain Sharing
Check this box to enable Domain Sharing. After you have enabled Domain Sharing and added all of the Domain Sharing hosts or IP addresses to the list, ensure that you have also enabled and configured Minger 640 so you can respond to queries from those hosts when they attempt to verify your local addresses.

Remove
To delete one of your Domain Sharing entries, select it from the list and click this button.

Host or IP
Use this box to enter the host or IP address that is sharing one or more of your domains. You can append a colon and port (e.g. `mail.example.com:2525`) if you wish to use a specific, non-default port when sending SMTP messages to the host (this is not the same as the Minger port below).

Minger port
This is the port that Minger will use when querying this host. The default port is 4069.

Minger password (optional)
If the host that you are adding requires a Minger password, enter it here. Setting up Minger to require a password is optional, but it is recommended.

Add
After entering the host or IP, port, and password, click this button to add the new Domain Sharing entry to the list.

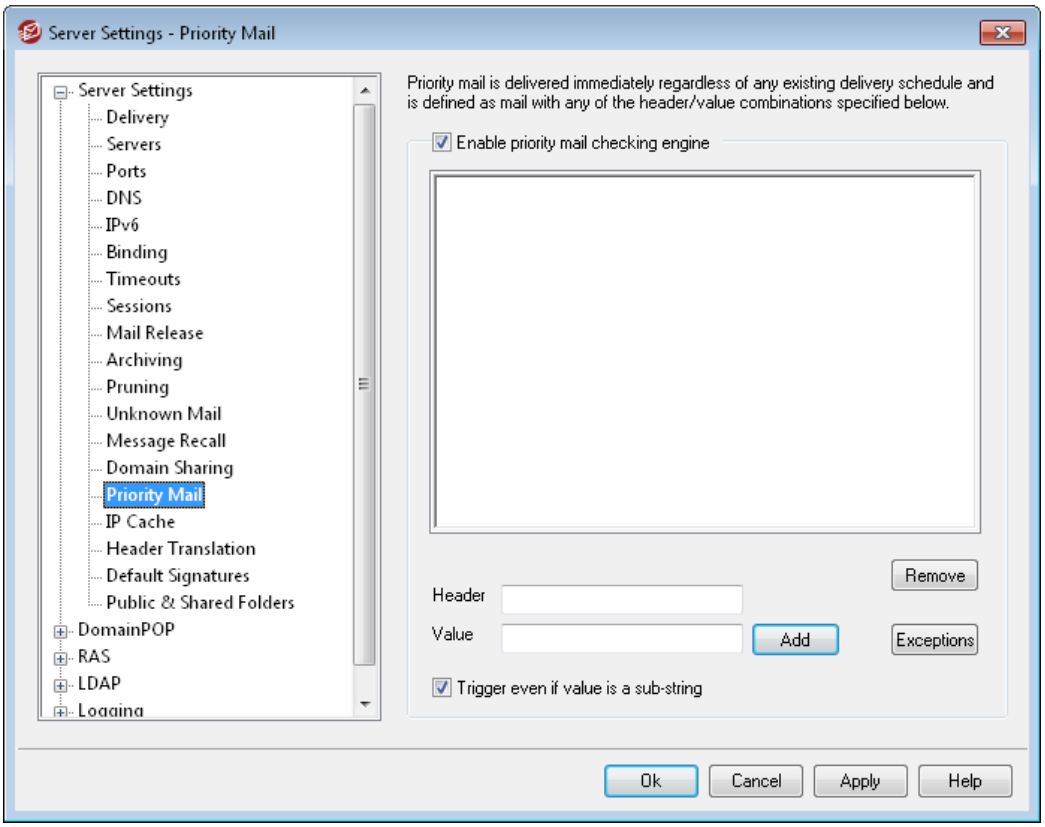
Do not send Domain Sharing mail to smart host on delivery errors
When this option is enabled, if MDaemon encounters an error while attempting to deliver Domain Sharing email (e.g. such as when the Domain Sharing host is offline), the email will be kept in the queue 654 rather than sent to the smart host 50. Sending these emails to the smart host can often lead to a mail loop. This option is enabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Minger 640
Domain Manager 121

3.1.1.15 Priority Mail



The Priority Mail screen is reached from the "Setup » Server Settings » Priority Mail" menu selection. It is used to define what constitutes Priority Mail on your system. Priority mail is delivered immediately by MDaemon regardless of scheduled mail processing intervals. When a new message arrives, MDaemon inspects its headers for a set of header/value combinations that you have specified on this dialog. If it finds them, it considers the message a high priority item and attempts to deliver it immediately.

Priority Mail Engine

Enable priority mail checking engine
Check this box to enable the Priority Mail feature. MDaemon will inspect incoming messages for priority status.

Header
Enter the message header in this field. Do not include the ending colon character.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Value
Enter the value that must be found in the specified header in order for the message to be considered high priority.

Trigger even if value is a sub-string
When entering a new Priority Mail setting you may select this feature to enable priority matching of a portion (or sub-string) of a header value. For example, you could create a Priority Mail Setting for the "`To`" header with the value "`Boss`". Then, any email containing "`Boss@anything`" in that header would be considered Priority Mail. If an entry is created without this feature enabled then the value of the header must match the entry exactly; matching only a portion will not be sufficient.

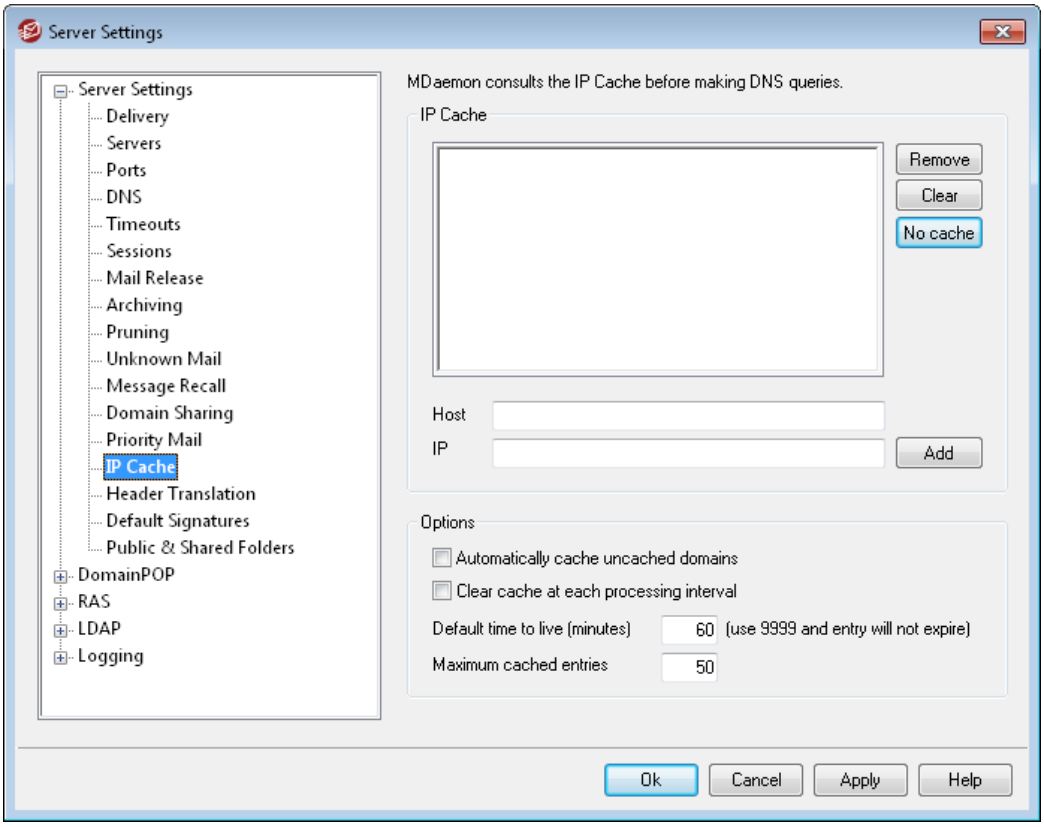
Add
After entering the Header/Value information in the specified text boxes, and after specifying whether this entry will apply to sub-strings, click the *Add* button to create the new Priority Mail entry.

Remove
Click this button to remove a selected entry from the *Current Priority Mail Settings* window.

Exceptions
This allows you to define field/value combinations that will cause a message to be considered an exception to the priority mail settings. This gives you more flexible control over this feature.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.16 IP Cache



In order to speed message delivery and shorten mail processing time, MDaemon caches the IP addresses of all hosts with which it comes in contact. These IPs are stored and then the cache is checked each time MDaemon requires a DNS resolution on a host name. If the host name needing resolution is found in the IP cache then the DNS lookup is skipped, which can save a surprising amount of processing time. The settings in this window allow you to manipulate the parameters under which the cache will operate. You may also manually add and remove entries, set the maximum size of the cache, and designate how long entries will remain cached. The IP Cache can be reached from the "Setup » Server Settings » IP Cache" menu selection.

IP Cache

Host
Enter the host that you wish to add to the IP cache.

IP
Enter the IP address that you wish to add to the IP cache.

Add
Once you have manually entered a host and IP address, click this button to add it to the cache.

Remove
If you wish to remove a cached IP address from the list, select the entry and then

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

click this button.

Clear
This button will delete all entries in the cache.

No cache
Click this button to bring up a list of domain names and/or IP addresses that you never want MDaemon to add to the IP Cache.

Settings

Automatically cache uncached domains
This option governs MDaemon's internal auto-caching engine. If you want MDaemon to cache domains automatically then enable this option. If you want to build the IP Cache yourself, then clear this checkbox.

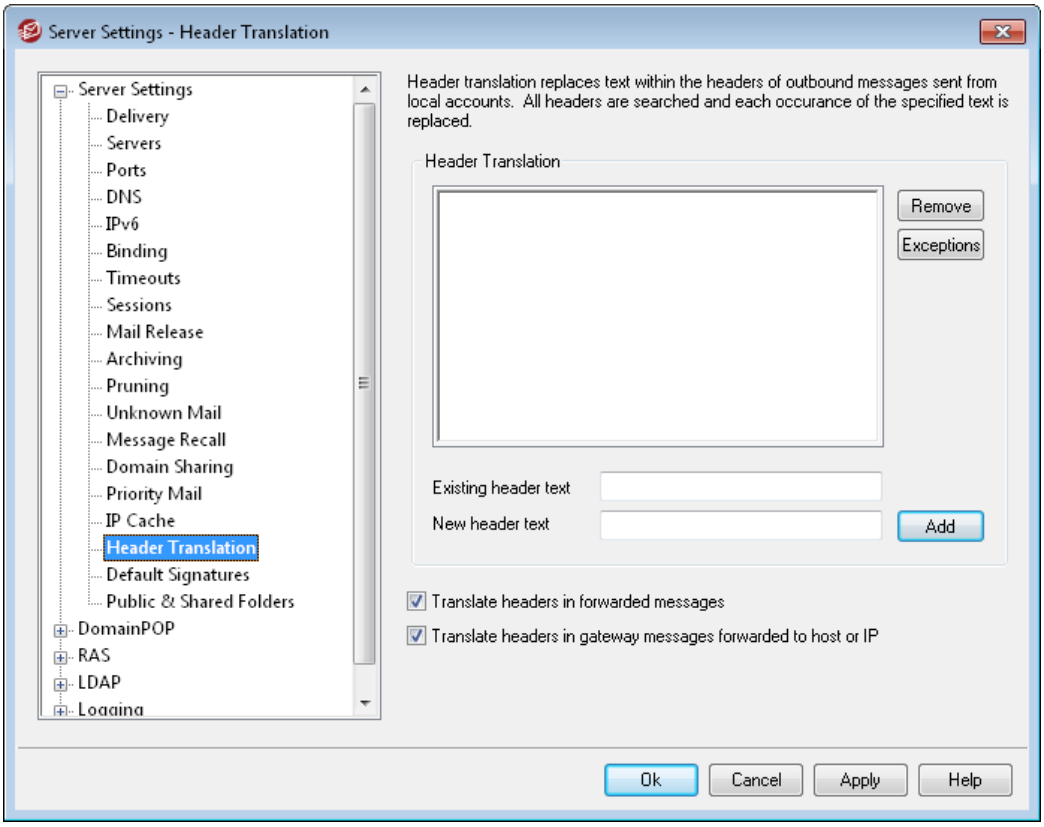
Clear cache at each processing interval
If selected, the entire contents of the cache will be flushed at the start of each mail session. This allows the cache to be refreshed at each processing interval.

Default time to live (minutes)
This is the default value in minutes that an entry will remain in the IP Cache. Once the entry has been in the IP Cache for this number of minutes, MDaemon will remove it. If you want to set a permanent entry in the IP Cache then designate the *Default time to live* as 9999.

Max cached entries
This value determines how large the cache may be. Once this number is reached, the next cache entry will bump the first one out of the cache.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.17 Header Translation



The Header Translation feature can change any portion of text found within a header to a new value whenever a message is detected which must leave your domain destined for a remote host. You specify the text you want to search for and its corresponding replacement value. MDaemon will then search through all the headers in the message and make the replacements. You may also specify headers that MDaemon should **not** modify (such as "Subject:" or "Received:" headers) by clicking the *Exceptions* button on this dialog.

This feature is necessary for some MDaemon configurations in which the local domain name is fictitious or different from the domain name that must appear on outbound mail. In such a situation, Header Translation could be used to change every occurrence of "`@localdomain`" to "`@RemoteDomain`".

Header Translations

This list contains the portions of text that MDaemon will scan for in the outbound message headers, and the text that will be substituted when a match is found.

Remove
Select an entry in the Current Header Translations list and then click this button to remove it from the list.

Exceptions
Click this button to open the Header Translation Exceptions 821 dialog. This dialog is

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

used for specifying any Headers that you wish to be omitted from the Header Translation process.

Existing header text
Type the text that you want to be replaced when it is found within the headers of any outbound message.

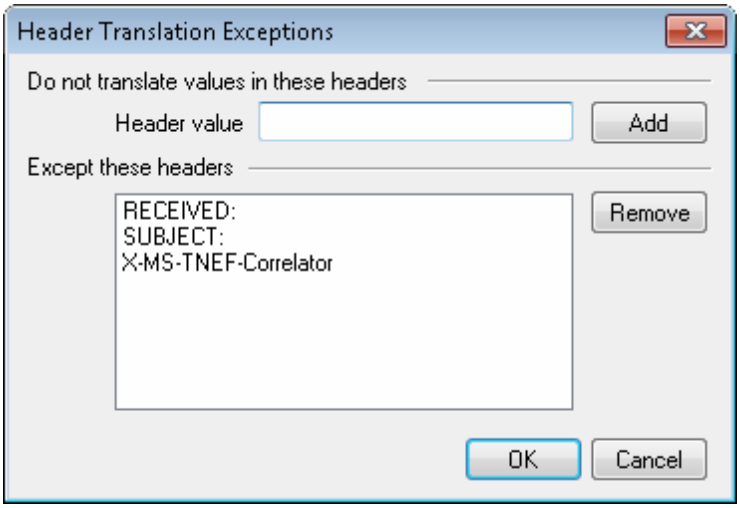
New header text
This text will be substituted for that which you specified in the *Existing header text* field.

Add
Click this button to add the above text parameters to the *Header Translation* list.

Translate headers in forwarded messages
Click this checkbox to cause the header translations to apply also to messages automatically forwarded from a local domain to a non-local domain.

Translate headers in gateway messages forwarded to host or IP
Click this check box if you want the headers to be translated in forwarded domain gateway mail. See the Forwarding 174 screen of the Gateway Editor for more information.

3.1.1.17.1 Header Translation Exceptions



Do not translate values in these headers

Header value
Enter any header that you want to be omitted from the Header Translation 81 process.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

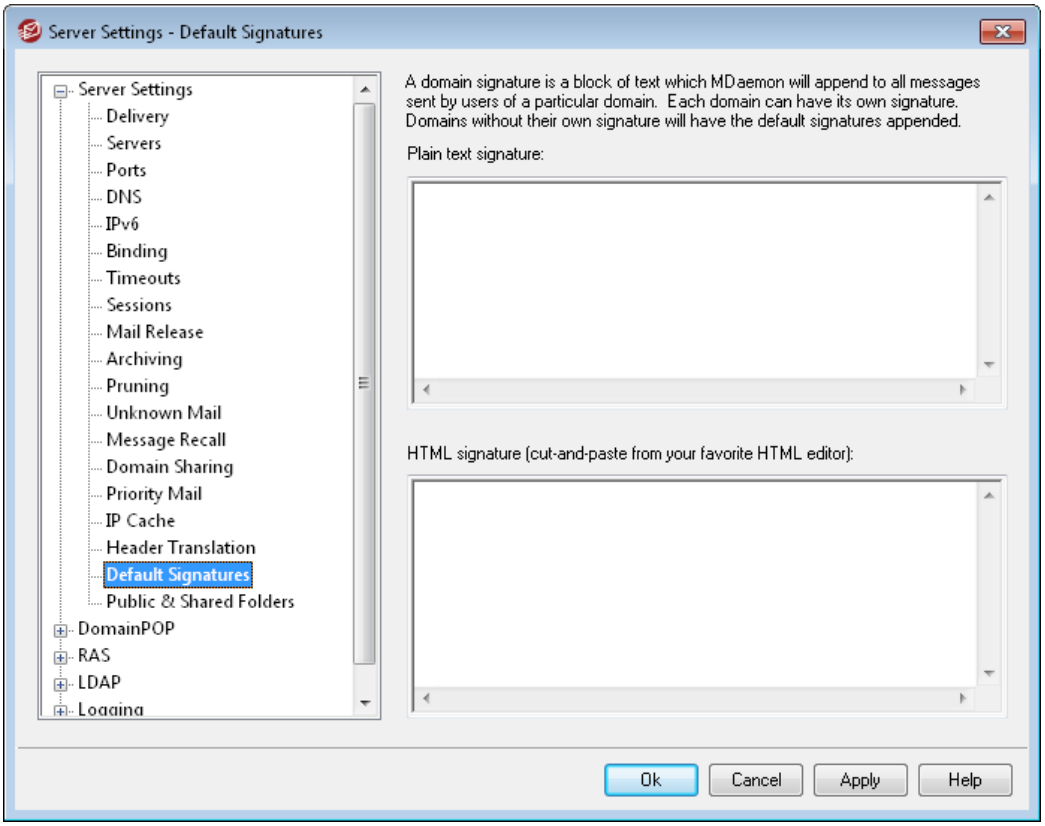
Add
Click this button to add a new header to the list.

Except these headers

MDaemon will not scan these headers when it is substituting header text.

Remove
Select a header in the list and then click this button to remove it.

3.1.1.18 Default Signatures



Use this screen to append a signature to all messages sent by your MDaemon users. Use the Signatures 138 screen on the Domain Manager if you wish to use a different signatures for users of specific domains—when a domain-specific signature exists it will be used instead of the Default Signature. Signatures are added to the bottom of messages, except for mailing list messages using a footer 206, in which case the footer is added below the Signature. You can also use the Account Editor's Signature 568 feature to add individual signatures for each Account. Account signatures are added just before Default or Domain Signatures.

Plain text signature

This area is for inserting a plain text signature. If you wish to designate a

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

corresponding html signature to be used in the text/html part of multipart messages, use the *HTML signature* area below. If a signature is included in both places then MDaemon will use the appropriate one for each part of the multipart message. If no html signature is specified then the plain text signature will be used in both parts.

HTML signature (cut-and-paste from your favorite HTML editor)

This area is for inserting an HTML signature to be used in the text/html part of multipart messages. If a signature is included both here and in the *Plain text signature* area above, MDaemon will use the appropriate one for each part of the multipart message. If no html signature is specified then the plain text signature will be used in both parts.

To create your html signature, either type the html code here manually or cut-and-paste it directly from your favorite HTML editor. If you wish to include inline images in your HTML signature, you can do so by using the `$ATTACH_INLINE:path_to_image_file$` macro.

For example:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

There are also several ways you can insert inline images into Default and Domain Signatures[138] from within MDaemon's Remote Administration[251] web interface:

- On the Signature/Footer screen in Remote Administration, click the "Image" toolbar button in the HTML editor and select the upload tab
- On the Signature/Footer screen in Remote Administration, click the "Add image" toolbar button in the HTML editor.
- Drag and drop an image into the Signature/Footer screen's HTML editor with Chrome, FireFox, Safari, or MSIE 10+
- Copy and paste an image from the clipboard into the Signature/Footer screen's HTML editor with Chrome, FireFox, MSIE 11+

See:

Domain Manager » Signatures[138]
Account Editor » Signature[568]

3.1.1.19 Public & Shared Folders

MDaemon supports shared Public and User IMAP folders. Public folders (managed from the Public Folder Manager[218]) are extra folders that do not belong to any particular account but can be made available to multiple IMAP users. User folders are IMAP folders that belong to individual MDaemon accounts. Each shared folder, whether public or user, must have a list of MDaemon users associated with it, and only members of that access list may access it via WorldClient or an IMAP email client.

When IMAP users access their list of personal folders, they will also see the shared public and shared user folders to which they have been given access. In this way

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

certain mail folders can be shared by multiple users but still require each user's individual logon credentials. Further, having access to a folder doesn't necessarily mean having full read/write or administrative access to it. Specific access rights can be granted to individual users, thus allowing you to set different levels of access for each one. For example, you might allow some users to delete messages while restricting that from others.

Once a public or user IMAP folder has been created you can use the Content Filter to set criteria by which certain messages are moved into that folder. For example, it might be useful to make a filter rule that would cause messages containing `support@example.com` in the `TO:` header to be moved into the `Support` public folder. The Content Filter actions 366 "`Move Message to Public Folders...`" and "`Copy Message to Folder...`" make this possible. For shared user folders, you can use your personal IMAP filters 541 to route specific messages to them. In addition to using Content Filters and IMAP filters, you can associate a specific account with a shared folder so that messages destined for that "Submission Address" will be automatically routed to the shared folder. However, only users who have been granted "post" permission to the folder will be able to send to that address.

For added convenience, the Mailing List editor also contains a Public Folder 208 screen that makes it possible for you to configure a public folder for use with a particular list. If you enable this feature then a copy of each list message will be placed into the specified public folder. All public folders are stored in the `\Public Folders\` directory within the MDaemon directory hierarchy.

WorldClient Documents Folders

The WorldClient themes support document sharing using document folders. Document folders have full Access Control List (ACL) 220 support like other shared folders, which can be used to set permissions and sharing rules, and any types of files can be shared through the system. WorldClient users can upload files to their document folders using the built-in tools. When using the LookOut theme, browsers that support the HTML5 Drag and Drop API, such as Chrome and Firefox, can also upload files by dragging them from the desktop into the browser window. Filenames can be searched and renamed, and files can be attached to new messages that are being composed.

You can enable/disable the documents folders (and other shared folders) on a per-domain and per-user basis by editing the `\WorldClient\Domains.ini` file and individual `\Users\..\WC\user.ini` files respectively. You can configure both default settings and customized settings, which will override the defaults. For example:

```
[Default:UserDefaults]
DocumentsFolderName=Documents
EnableDocuments=Yes

[example.com:UserDefaults]
DocumentsFolderName=Example Documents
EnableDocuments=Yes

[superControllingDomain.gov:UserDefaults]
EnableDocuments=No
EnableCalendar=No
EnableNotes=No
EnableTasks=No
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Setting a Maximum File Size

You can limit the size of individual files that can be uploaded to documents folders by adding this key to the `domains.ini` file: `MaxAttachmentSize=<value in KB>` The default value is `0`, which means there is no limit.

Blocking or Allowing File Types

To prevent certain file types from being uploaded to the documents folder, add the `BlockFileTypes=` key to the `domains.ini` file, listing the files types you wish to block separated by a space or comma. For example, "`BlockFileTypes=exe dll js`".

To allow only certain file types to be uploaded to the documents folder, add the `AllowFileTypes=` key to the `domains.ini` file, listing the files types you wish to allow separated by a space or comma. For example, "`AllowFileTypes=jpg png doc docx xls xlsx`".

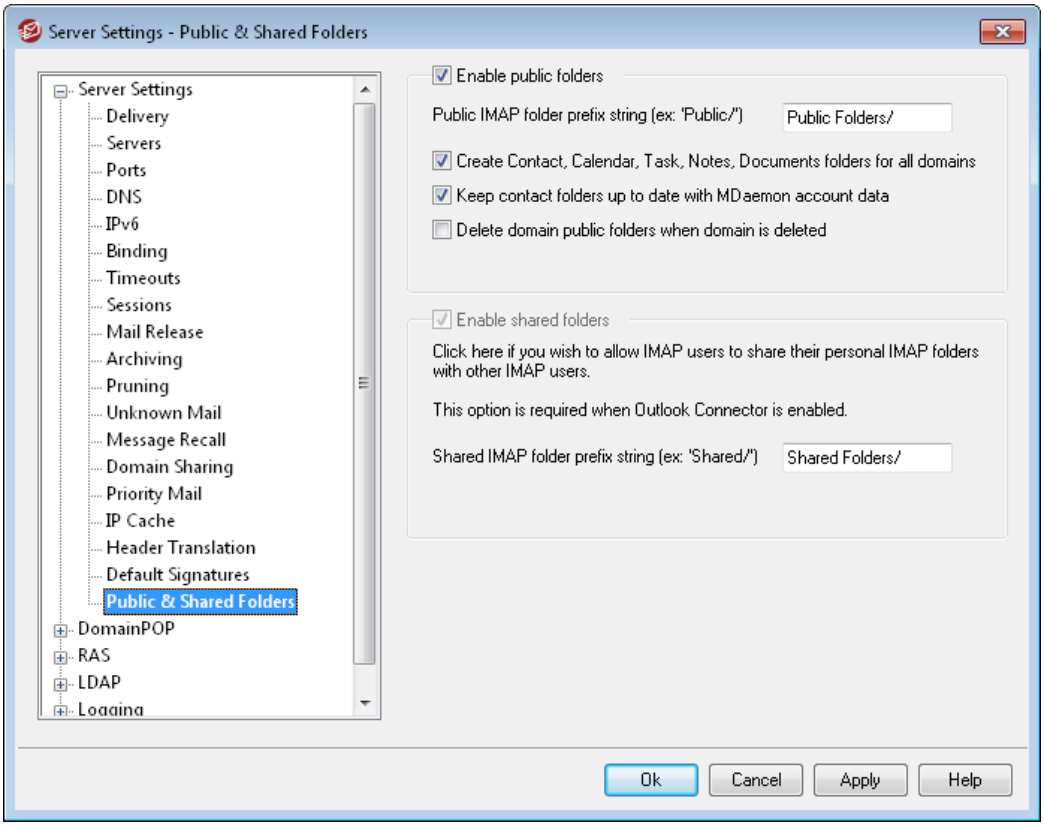
When both keys are used, priority is given to blocked files when there is a conflict; if an extension is in both lists then that extension will be blocked. If a key is used without a value (i.e. no list of extensions), then that key will not be used. File extensions can include a "." (e.g. .exe .dll), but it isn't required.

See:

Public & Shared Folders 87
Public Folder Manager 218
Access Control List 220
Account Editor » Shared Folders 547
Mailing List » Public Folders 208

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.1.19.1 Public & Shared Folders



To reach the Public & Shared Folders screen, click "Setup » Server Settings » Public & Shared Folders".

Enable public folders

Click this check box if you wish to allow users to gain access to public folders. The users that can access them and the level of access granted is designated under each folder on the Public Folder Manager[218]. Clear this check box if you want to hide public folders from all users.

Public IMAP folder prefix string (ex: 'Public/')
Public folders are prefixed with a sequence of up to 20 characters, such as "#" or "Public Folders/". This is to help users easily distinguish public from private folders from within their email client. Use this text box to specify the series of characters that you wish to use to denote public folders.

Create Contact, Calendar, Task, Journal, and Notes folders for all domains
Click this check box if you wish to ensure that these folders exist for all domains. Whenever a Domain[121] is added to MDaemon, these folders will be created.

Keep contact folders up to date with MDaemon account data
If this option is enabled, MDaemon will keep the contact folders synchronized with its account list.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Delete domain public folders when domain is deleted
Click this check box if you wish to delete a domain's public folders when the domain is deleted.

Enable shared folders

Click this check box if you wish to allow IMAP users to share access to their IMAP folders. The users who can access them and the level of access granted is designated under each folder on the Shared Folders 547 screen of the Account Editor (Accounts » Account Manager » [User Account] » Shared Folders). Clear this check box if you wish to prevent users from being able to share access to their folders, and prevent the aforementioned Shared Folders screen from appearing on the Account Editor.

When using Outlook Connector for MDaemon, this option will be unavailable. You will not be able to deactivate it because user folder sharing is required for Outlook Connector to function properly.

Shared IMAP folder prefix string (ex: 'Shared/')
Shared user folders are prefixed with a sequence of up to 20 characters, such as "Public Folders/". This is to help users easily distinguish shared from private folders from within their email client. Use this text box to specify the series of characters that you wish to use to denote shared user folders.

See:

Public Folders Overview 84
Public Folder Manager 218
Access Control List 220
Account Editor » Shared Folders 547
Mailing List » Public Folders 208

3.1.2 DomainPOP

Use DomainPOP Mail Collection ("Setup » Server Settings » DomainPOP") to configure MDaemon to download mail from a remote POP mailbox for redistribution to your users. This feature works by using the POP3 protocol to download all the mail found in the ISP's POP mailbox associated with the specified logon. Once collected, the messages are parsed according to the settings provided on this dialog and then placed in user mailboxes or the remote mail queue for MDaemon to deliver, just as if the messages had arrived at the server using conventional SMTP transactions.

It is important to note that messages stored in mailboxes and retrieved using the POP3 protocol will be devoid of the important routing information (sometimes called the message's "envelope") that would ordinarily be supplied had the messages been delivered using the more powerful SMTP protocol. Without this routing information, MDaemon is forced to "read" the message and examine the headers in an attempt to determine to whom the message was originally intended. This is not an exact science

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

to say the least. Message headers are sometimes notorious for their lack of sufficient information needed to determine the intended recipient. This lack of what would seem to be a fundamental characteristic of an email message - the recipient - may seem surprising but one must keep in mind that the message was never intended to be delivered to its recipient using the POP protocol. With SMTP, the contents of the message are irrelevant since the protocol itself dictates specifically to the server, during the mail transaction, the intended recipient of the message.

In order to allow for POP retrieval and delivery of mail messages in a reliable and consistent way, MDaemon employs a powerful suite of header processing options. When MDaemon downloads a message from a remote POP source it immediately parses all the relevant headers within that message and builds a collection of potential recipients. Every email address found in the headers that MDaemon inspects is included in the collection.

Once this process is complete, MDaemon's collection of recipients is divided into local and remote sets. Further, all addresses that are parsed and placed into the collection of potential recipients are processed through the Aliases 613 translator before being divided into local and remote sets. Every member of the local set (addresses with a domain that matches one of MDaemon's local domains) will receive a copy of the message. What happens to the remote set is governed by the settings in this dialog. You can elect to simply ignore these addresses, forward a summary listing of them to the postmaster, or honor them — in which case MDaemon will actually deliver a copy of the message to the remote recipient. Only under rare circumstances would the need to deliver these messages to remote recipients be warranted.

Care must be taken to prevent duplicate messages or endlessly looping mail delivery cycles. A common problem that results from the loss of the SMTP envelope manifests itself with mailing list mail. Typically, messages distributed by a mailing list do not contain within the message body any reference to the addresses of the recipients. Rather, the list engine simply inserts the name of the mailing list into the `TO:` field. This presents an immediate problem: if the `TO:` field contains the name of the mailing list then the potential exists for MDaemon to download this message, parse the `TO:` field (which will yield the name of the mailing list), and then dispatch the message right back to the same list. This would in turn deliver another copy of the same message back to the POP mailbox from which MDaemon downloaded the original message — thus starting the whole cycle over again. To cope with such problems mail administrators must take care to use the tools and settings that MDaemon provides to either delete mailing list mail or perhaps alias it in such a way that it will be delivered to the proper local recipient(s). You could also utilize the Routing Rules or Content Filters to deliver the message to the correct recipient(s).

Additional concerns when employing this sort of mail collection scheme revolve around the issue of unwanted message duplication. It is very easy for mail that is delivered to the ISP's POP mailbox using SMTP to generate unwanted duplicates, once it has been collected using DomainPOP. For example, suppose a message is sent to someone at your domain and a carbon copy is sent to another person at the same domain. In this situation, SMTP will deliver **two** copies of the same message to your ISP's mailbox — one for each recipient. Each of the two message files will contain references to **both** recipients — one in the `TO:` field and the other in the `CC:` field. MDaemon will collect each of these two identical message files and parse both addresses from each of them. This would result in both recipients receiving one unwanted duplicate message. To guard against this sort of duplication MDaemon uses a control which allows you to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

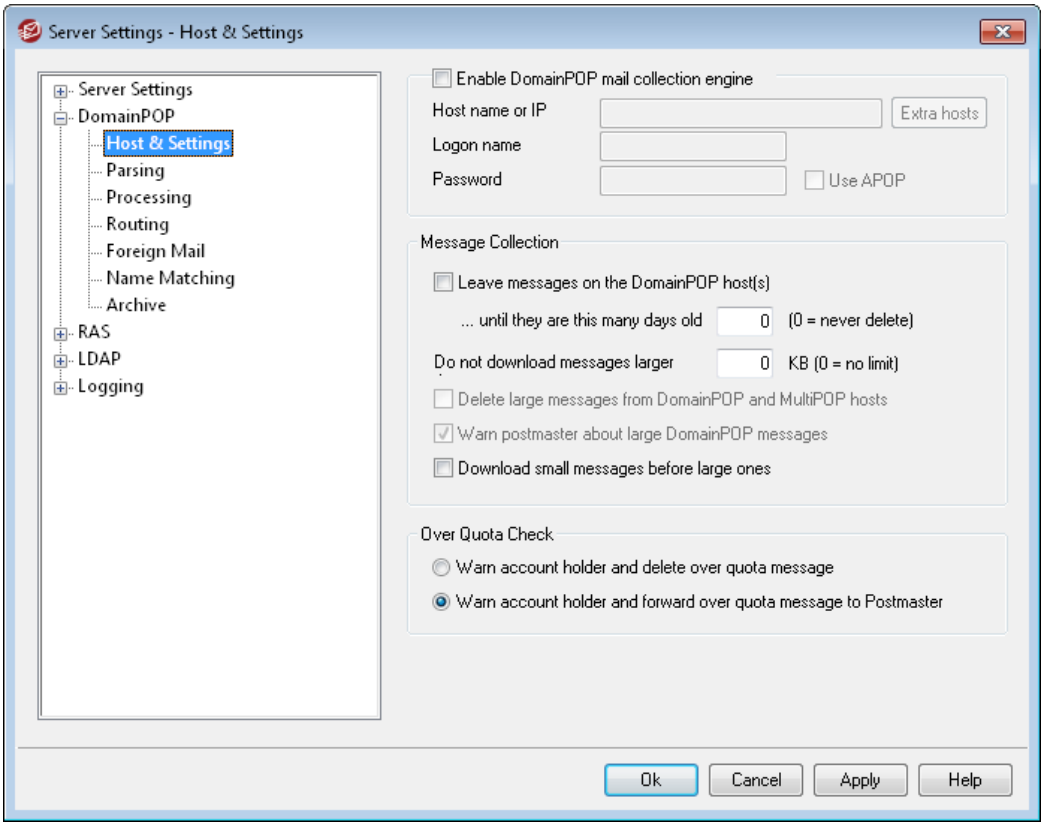
specify a header that MDaemon will use to check for duplication. The `Message-ID` field is ideal for this. In the above example, both messages are identical and will therefore contain the same `Message-ID` field value. MDaemon can use this value to identify and remove the second message during the download stage before it can be parsed for address information.

As a final measure guarding against duplicate messages and endless looping delivery cycles, MDaemon employs a means for detecting how many trips or "hops" a message has made through the transport system. Each time an SMTP mail server processes a message it "stamps" the message with a "Received" header. MDaemon counts all such headers when it encounters a message for the first time. If the total number of mail servers exceeds a specified value, it is likely the message is caught in a delivery loop and should be taken out of the mail stream and moved to the bad message directory. This value can be configured under the Retry Queue 654.

See:

Content Filters 362
Mailing Lists 180

3.1.2.1 Host & Settings



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

DomainPOP Host Properties

Enable DomainPOP mail collection engine
If selected, MDaemon will use the setting provided on this screen to collect mail from a DomainPOP mail host for local redistribution.

Host name or IP
Enter your DomainPOP host's domain name or IP address here.

Extra hosts
Click this button to open the `DpopXtra.dat` file, on which you can designate extra hosts from which to collect DomainPOP mail. See the contents of that file for more information.

Logon name
Enter your login of the POP account used by DomainPOP.

Password
Enter the POP or APOP account's password here.

Use APOP
Click this box if you wish to use the APOP command and CRAM-MD5 authentication when retrieving your mail. This makes it possible to authenticate yourself without having to send clear text passwords.

Message Collection

Leave messages on the DomainPOP host(s)
If selected, MDaemon will download but not remove the messages from your DomainPOP mail host.

...until they are this many days old (0=never delete)
This is the number of days that a message can remain on the DomainPOP host before it will be deleted. Use "0" if you do not wish to delete older messages.

Some hosts may limit the amount time that you are allowed to store messages in your mailbox.

Don't download messages larger than [XX] KB (0 = no limit)
Messages greater than or equal to this size will not be downloaded from your DomainPOP mail host. Enter "0" if you want MDaemon to download messages no matter the size.

Delete large messages from DomainPOP and MultiPOP hosts
Enable this option and MDaemon will delete messages that exceed the size designated above. The messages will simply be removed from the DomainPOP and MultiPOP mail hosts and will not be downloaded.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Warn postmaster about large DomainPOP messages
Check this option and MDaemon will send a warning to the postmaster whenever a large message is discovered in the DomainPOP mailbox.

Download small messages before large ones
Enable this checkbox if you want the message downloading order to be based on size — beginning with the smallest and proceeding to the largest.

This option retrieves smaller messages quicker but requires a larger amount of internal sorting and processing.

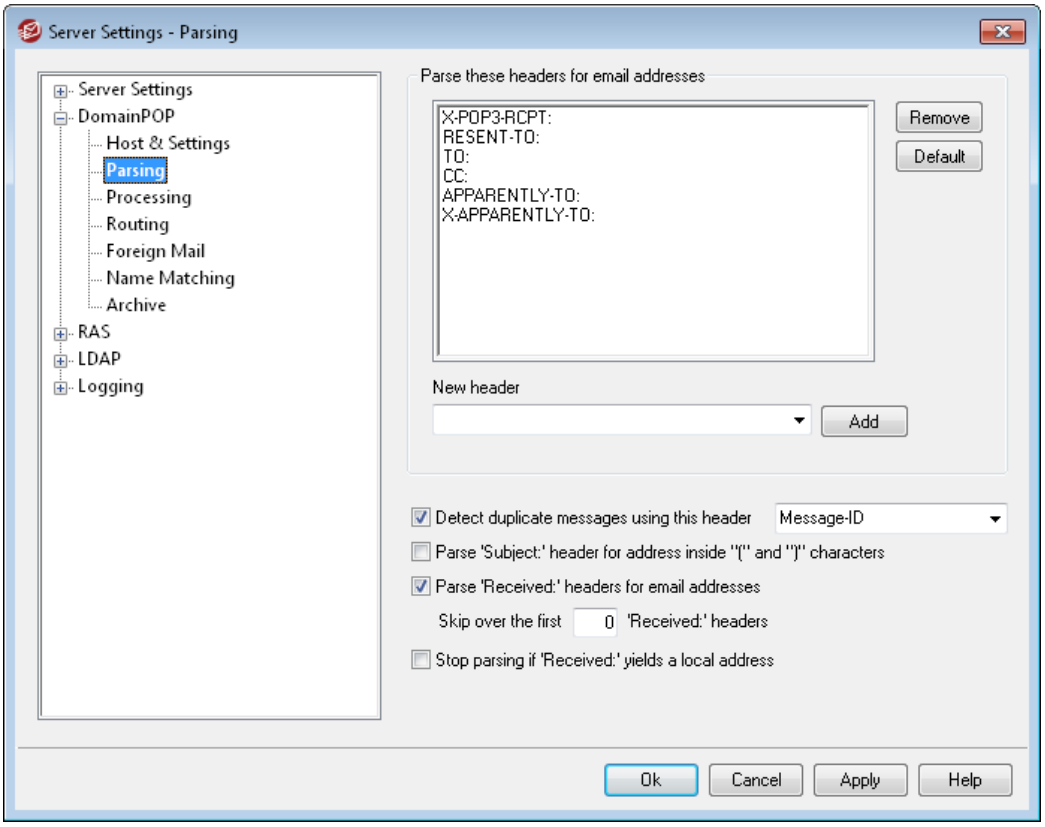
Over Quota Check

Warn account holder and delete over quota message
When this option is chosen and a message is collected for an account that is over its quota (designated on the Quotas 537 screen of the account editor), MDaemon will delete the message and then send a message to the account holder stating that the account is over its limit.

Warn account holder and forward over quota message to Postmaster
When this option is chosen and a message is collected for an account that is over its quota, MDaemon will forward the message to the Postmaster and send a warning to the user letting him or her know that the account is over its limit.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.2.2 Parsing



Parse these headers for email addresses

This area lists the headers that MDaemon will parse in an attempt to extract addresses. Every header listed here is checked for addresses.

Remove
This button will remove the selected entries from the header list.

Default
This button will clear the current contents of the header list and add MDaemon's default list of headers. The default headers are typically sufficient to extract all addresses from the message.

New header
Enter the header you wish to add to the header list.

Add
After specifying a header in the *New header* option, click this button to add it to the list.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Delete duplicated messages using this header
If this option is selected MDaemon will remember the value of the specified header and will not process additional messages collected in the same processing cycle which contain an identical value. The `Message-ID` header is the default header used by this option.

Parse "subject:" header for address inside "(" and ")" characters
When this is selected and MDaemon finds an address contained in "( )" in the "Subject:" header of a message, this address will be added to the message's list of recipients along with any other parsed addresses.

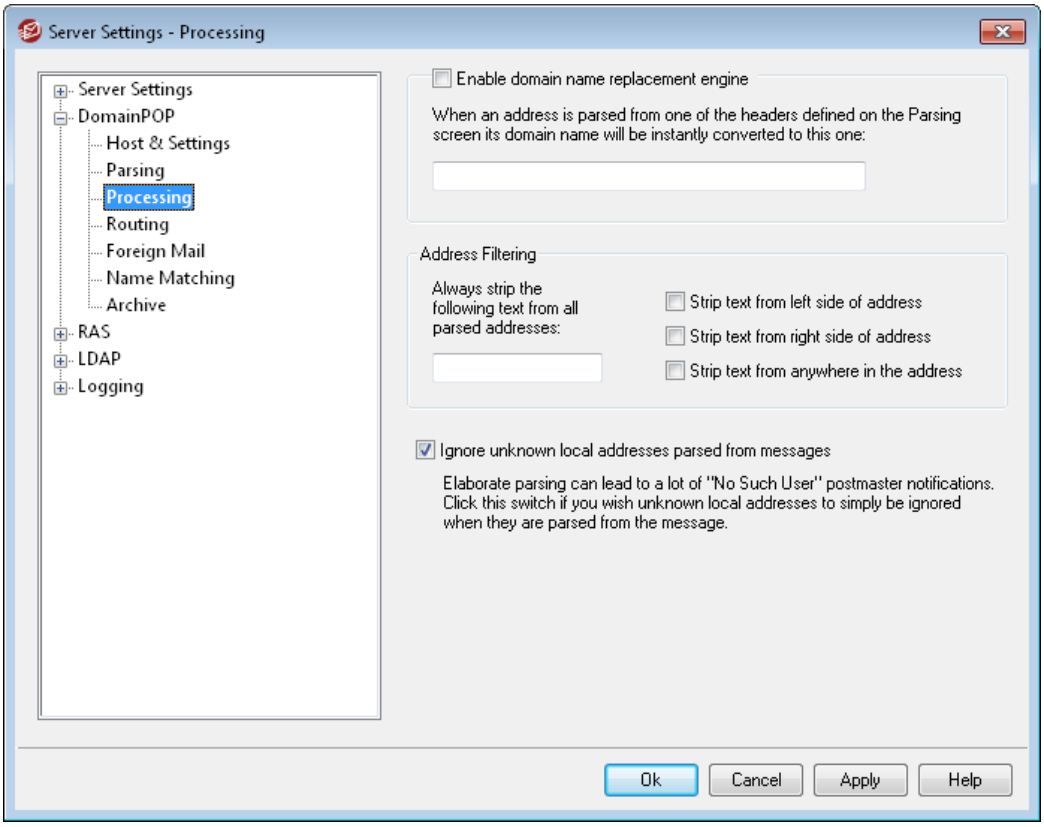
Parse "Received" headers for email addresses
It is possible to store the recipient information ordinarily found only within the message's envelope in the "Received" message headers. This makes it possible for parsers of the mail message to be able to glean the actual recipient address by merely inspecting the Received headers later. Click this checkbox if you wish to parse valid addresses from all of the "received" headers found within the mail message.

Skip over the first xx "received" headers
In some server configurations you may wish to parse Received headers but need to skip the first few of them. This setting allows you to enter the number of "Received" headers that MD will skip over before beginning its parsing.

Stop parsing if "Received" yields a valid local address
If while parsing a "received" header MDaemon detects a valid local address, this switch will cause all further parsing to stop and MDaemon will not search the message for more potential delivery addresses.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.2.3 Processing


Server Settings - Processing
Server Settings
DomainPOP
Host & Settings
Parsing
Processing
Routing
Foreign Mail
Name Matching
Archive
RAS
LDAP
Logging
Enable domain name replacement engine
When an address is parsed from one of the headers defined on the Parsing screen its domain name will be instantly converted to this one:
Address Filtering
Always strip the following text from all parsed addresses:
Strip text from left side of address
Strip text from right side of address
Strip text from anywhere in the address
Ignore unknown local addresses parsed from messages
Elaborate parsing can lead to a lot of "No Such User" postmaster notifications. Click this switch if you wish unknown local addresses to simply be ignored when they are parsed from the message.
Ok
Cancel
Apply
Help

Domain Name Replacement

Enable domain name replacement engine
This option can be used to reduce the number of aliases your site might require. When a message is downloaded, all domain names in all addresses parsed from that message will be converted to the domain name specified here.

Address Filtering

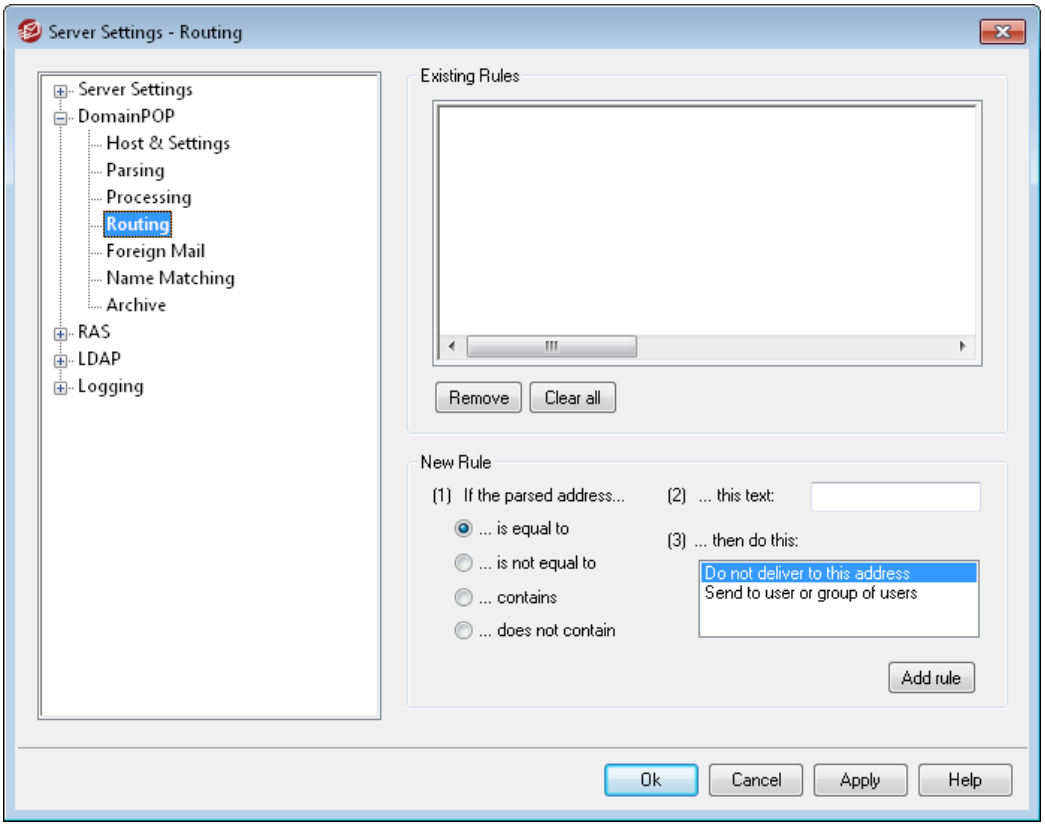
Always strip the following text from all parsed addresses
Some hosts will stamp each message with a line that indicates who the recipient of the message should be, along with a bit of routing information appended to the address on either the left or right side. This stamp would be perfect to use for parsing the recipient address except that the additional routing information makes this impossible without a lot of account aliasing. Rather than do all that you can simply specify the value of this appended text in the edit control associated with this feature and MDaemon will strip any occurrence of this text from all addresses that it parses.

Ignore unknown local addresses parsed from messages
As mentioned above, the Domain Name Replacement feature will alter the domain name in all email addresses parsed from a message, converting it into the one you

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

specify on this screen. This could create some addresses that do not have a corresponding account your server. Because the domain name but not the mailbox would be valid, MDaemon would consider such addresses unknown local users. Such mail typically generates a "No Such User" message. Check this box if you wish to prevent the Domain Name Replacement Engine from causing these messages to be generated.

3.1.2.4 Routing



Existing Rules

This list shows you the rules that you have created and will be applied to your messages.

Remove

Select a rule from the list and then click this button to delete it.

Clear all

This button removes all existing rules.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

New Rule

(1) If the parsed address...

Is equal to, is not equal to, contains, does not contain
This is the type of comparison that will be made when an address is compared to this routing rule. MDaemon will search each address for the text contained in the *"...this text*" option below and then proceed based upon this option's setting — does the address's complete text match exactly, not match exactly, contain the text, or not contain it at all?

(2) ...this text:
Enter the text that you want MDaemon to search for when scanning the addresses.

(3) ...then do this:
This option lists the available actions that can be performed if the result of the rule is true. You can choose from the following actions:

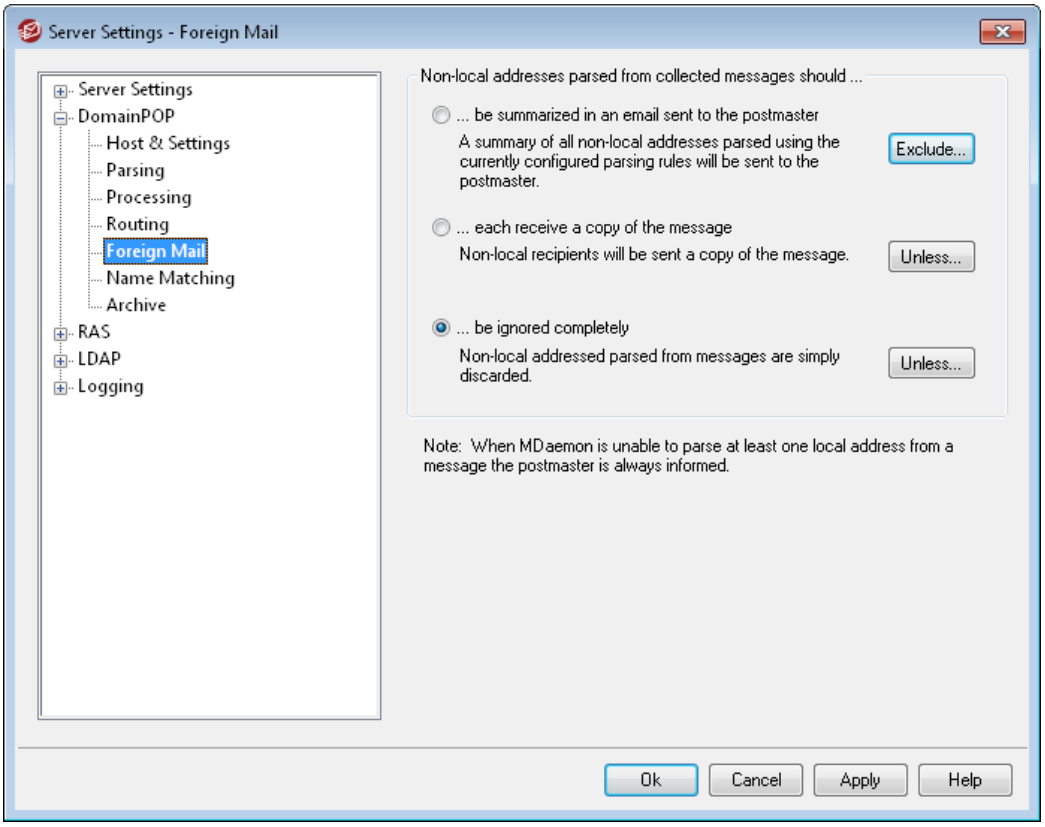
Do not deliver to this address - Selecting this action will prevent the message from being delivered to the specified address.

Send to user or group of users - Selecting this action will open dialog on which you can designate a list of email addresses that should receive a copy of the message being processed.

Add rule
After setting the new rule's parameters, click *Add rule* to add it to the list of rules.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.2.5 Foreign Mail


Server Settings - Foreign Mail
Server Settings
DomainPOP
Host & Settings
Parsing
Processing
Routing
Foreign Mail
Name Matching
Archive
RAS
LDAP
Logging
Non-local addresses parsed from collected messages should ...
... be summarized in an email sent to the postmaster
A summary of all non-local addresses parsed using the currently configured parsing rules will be sent to the postmaster.
Exclude...
... each receive a copy of the message
Non-local recipients will be sent a copy of the message.
Unless...
... be ignored completely
Non-local addressed parsed from messages are simply discarded.
Unless...
Note: When MDaemon is unable to parse at least one local address from a message the postmaster is always informed.
Ok
Cancel
Apply
Help

Non-local addresses parsed from collected messages should...

...be summarized in an email sent to the postmaster
If this option is selected MDaemon will send a single copy of the message to the postmaster along with a summary of the non-local addresses that the parsing engine extracted using the current set of headers and parsing rules.

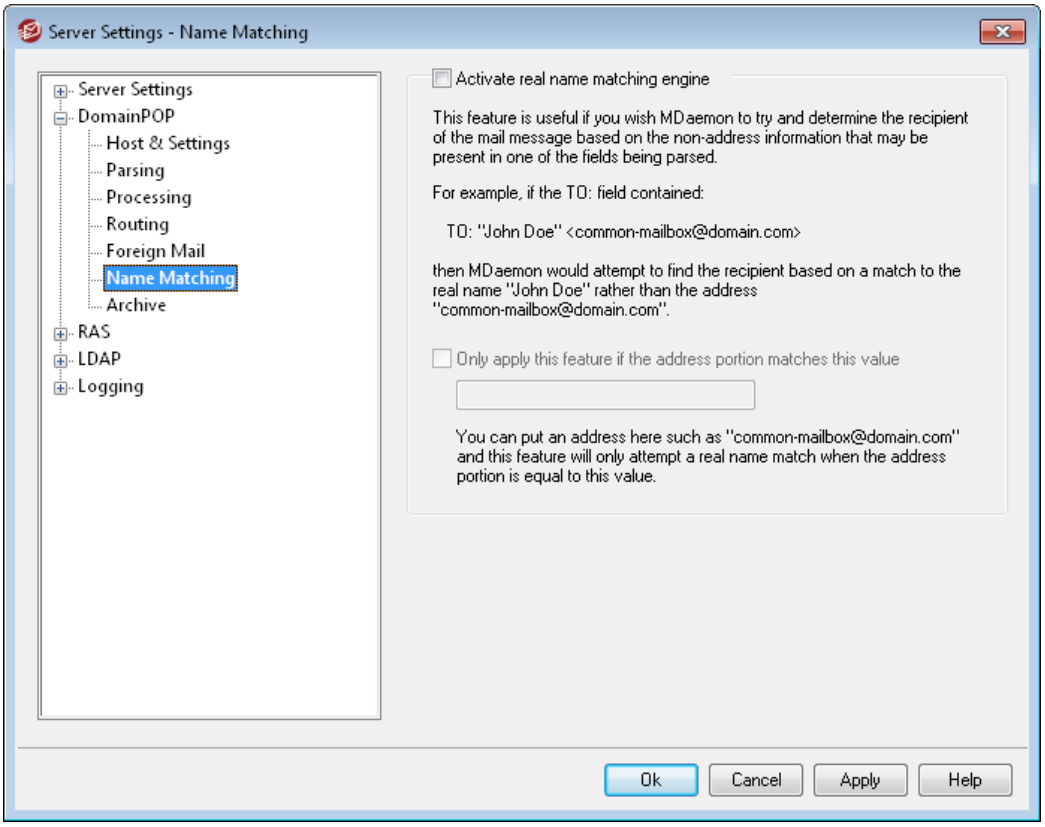
...each receive a copy of the message
If this option is selected MDaemon will deliver a copy of the message to any non-local recipient that it finds within the inspected headers.

...be ignored completely
If this option is selected MDaemon will remove from the recipient list any address that is non-local. It will be as if MDaemon never parsed remote addresses from the original downloaded message.

The *Exclude...* and *Unless...* buttons allow you to define addresses that will be treated as exceptions to the the selected option.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.2.6 Name Matching


Server Settings - Name Matching
Server Settings
DomainPOP
Host & Settings
Parsing
Processing
Routing
Foreign Mail
Name Matching
Archive
RAS
LDAP
Logging
Activate real name matching engine
This feature is useful if you wish MDaemon to try and determine the recipient of the mail message based on the non-address information that may be present in one of the fields being parsed.
For example, if the TO: field contained:
TO: "John Doe" <common-mailbox@domain.com>
then MDaemon would attempt to find the recipient based on a match to the real name "John Doe" rather than the address "common-mailbox@domain.com".
Only apply this feature if the address portion matches this value
You can put an address here such as "common-mailbox@domain.com" and this feature will only attempt a real name match when the address portion is equal to this value.
Ok
Cancel
Apply
Help

The Name Matching feature is only active in conjunction with the DomainPOP Mail Collection engine. If you wish to use this feature, you must make sure that you have DomainPOP enabled. DomainPOP can be reached from the "Setup » Server Settings » DomainPOP" menu selection.

Real Name Matching Engine

Activate real name matching engine
This feature allows MDaemon to determine who should receive a DomainPOP collected message based not upon the parsed email address but upon the text included with the address. This is typically the recipient's real name.

For example, a message's TO header might read:

```
TO: "Michael Mason" <user01@example.com>
```

or

```
TO: Michael Mason <user01@example.com>
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

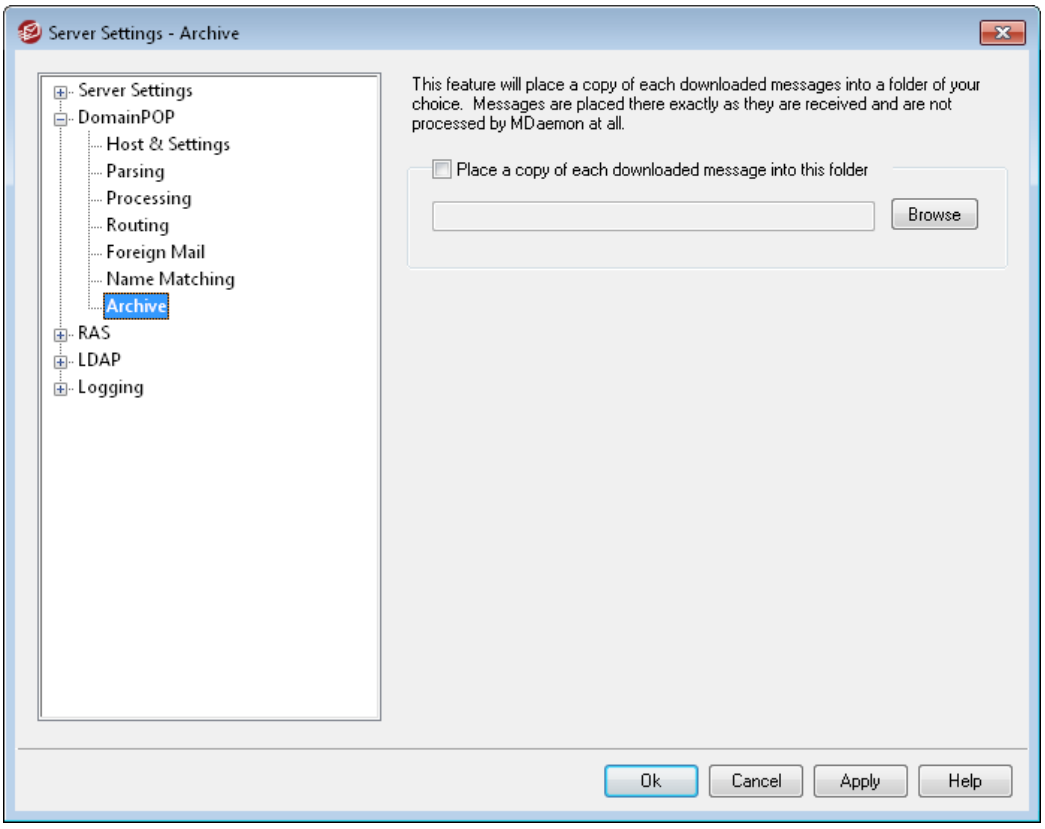
Name Matching ignores the "user01@example.com" portion of the address. It instead extracts the "Michael Mason" portion and checks to see if this is an MDaemon user. If a match is found to an account's real name then that account's local email address is used for delivery purposes. If no match is made then MDaemon reverts to delivering the message to the email address parsed from the data (user01@example.com in this example).

The real name portion of the address may not contain a comma, semi-colon, or colon character.

Only apply this feature if the address portion matches this value
This option allows you to specify an email address that must be present in the extracted data in order for the real name matching process to proceed. This allows you a measure of control over when the Name Matching feature will be employed. For example, you can specify an address such as "user01@example.com" and then only addresses matching this value will be candidates for Name Matching.

Suppose you specify "user01@example.com" in this option. This means that "`TO: 'Michael Mason' <user01@example.com>`" will be a candidate for Name Matching while "`TO: 'Michael Mason' <user02@example.com>` will not.

3.1.2.7 Archive



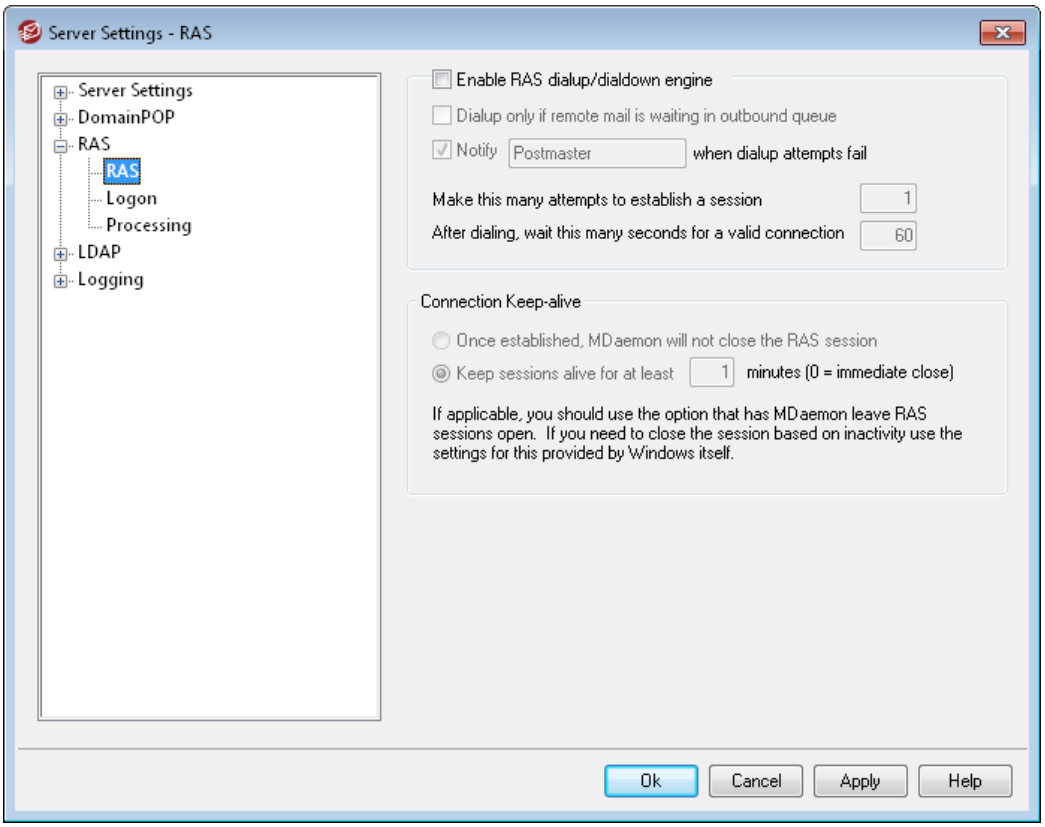
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Archive

Place a copy of each downloaded message into this folder
This is a safety feature to ensure that you don't lose any mail due to unforeseen parsing or other errors that might occur when downloading mail in bulk quantities. Check this box if you wish to save a copy of each downloaded message into the folder that you specify. These copies are placed in the folder exactly as they are received and are not processed by MDaemon at all.

3.1.3 RAS Dialup Settings

3.1.3.1 RAS


Server Settings - RAS
Server Settings
DomainPOP
RAS
RAS
Logon
Processing
LDAP
Logging
Enable RAS dialup/dialdown engine
Dialup only if remote mail is waiting in outbound queue
Notify
Postmaster
when dialup attempts fail
Make this many attempts to establish a session
1
After dialing, wait this many seconds for a valid connection
60
Connection Keep-alive
Once established, MDaemon will not close the RAS session
Keep sessions alive for at least
1
minutes (0 = immediate close)
If applicable, you should use the option that has MDaemon leave RAS sessions open. If you need to close the session based on inactivity use the settings for this provided by Windows itself.
Ok
Cancel
Apply
Help

Click the "Setup » Server Settings » RAS" menu selection to configure your RAS Dialup settings. This dialog will only be available if you have Remote Access Services installed on your system. It is used by MDaemon when you need to dial up your ISP just prior to a Remote Mail processing event.

Enable RAS dialup/dialdown engine
When this option is enabled, MDaemon will use the settings specified here to make a connection to a remote host before sending or receiving remote mail.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Dialup only if remote mail is waiting in outbound queue
When this box is checked, MDaemon will not dial the ISP unless there is remote mail waiting in the Remote queue. This may be beneficial in some circumstances but be aware that if MDaemon does not dial up then it cannot do any mail **collecting** either (unless it is delivered across the local LAN).

Notify [address] when dialup attempts fail
When selected, MDaemon will send a message to the specified address when a dialup event fails because of some error.

Make this many attempts to establish a session
MDaemon will attempt to connect to the remote host this many times before giving up.

After dialing, wait this many seconds for a valid connection
This value determines how long MDaemon will wait for the remote computer to answer and complete the RAS connection.

Connection Keep-alive

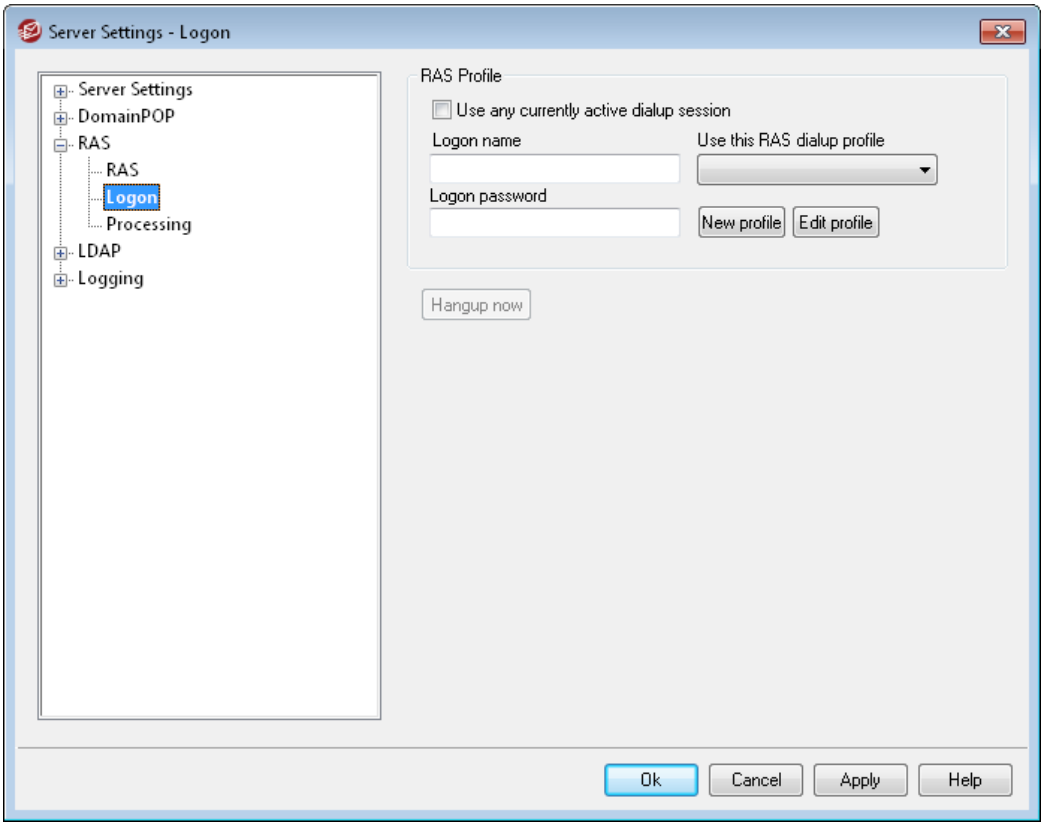
Once established, MDaemon will not close the RAS session
By default, MDaemon will shut down a created connection immediately after all mail transactions have been completed and the session is no longer in use. Selecting this option will cause the connection to remain open even after all transactions have been completed.

MDaemon will never close a connection that it did not create.

Keep sessions alive for at least xx minutes
If enabled, this option will cause an MDaemon created RAS session to remain open for at least the number of minutes specified or until all mail transactions have been completed, whichever is greater.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.3.2 Logon



RAS Profile

Use any currently active dialup session
Click this checkbox if you want MDaemon to be able to utilize other connection profiles when it detects that one is active. Whenever it is time to dialup, MDaemon will first check to see if there is an active connection that it can use rather than dialing.

Logon name
The value specified here is the user identification or login name that will be passed to the remote host during the authentication process.

Logon Password
The value specified here is the password that will be passed to the remote host during the authentication process.

Use this RAS dialup profile
This drop-down list box allows you to select a session profile that has been previously defined through windows Dialup Networking or Remote Access Services Setup.

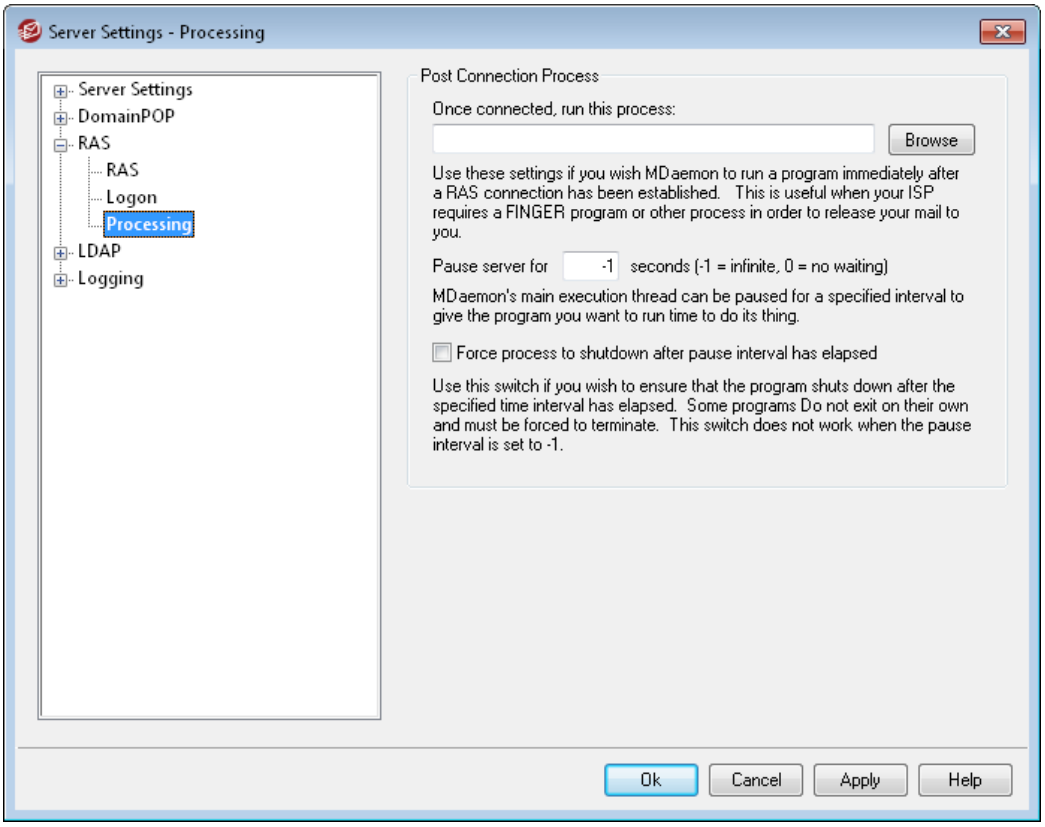
New profile
Click this button to create a new Dialup Networking or Remote Access Services profile.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Edit profile
Click this button to edit the currently selected Dialup Networking or Remote Access Services profile.

Hangup now
This button will close the connection to the ISP. This button is active only when MDaemon initiated the RAS session.

3.1.3.3 Processing


Server Settings - Processing
Server Settings
DomainPOP
RAS
RAS
Logon
Processing
LDAP
Logging
Post Connection Process
Once connected, run this process:
Browse
Use these settings if you wish MDaemon to run a program immediately after a RAS connection has been established. This is useful when your ISP requires a FINGER program or other process in order to release your mail to you.
Pause server for -1 seconds (-1 = infinite, 0 = no waiting)
MDaemon's main execution thread can be paused for a specified interval to give the program you want to run time to do its thing.
Force process to shutdown after pause interval has elapsed
Use this switch if you wish to ensure that the program shuts down after the specified time interval has elapsed. Some programs Do not exit on their own and must be forced to terminate. This switch does not work when the pause interval is set to -1.
Ok
Cancel
Apply
Help

Post Connection Process

Once connected, run this process
If a program is specified here, MDaemon will spawn a thread and execute the process. This is useful for those who require `Finger` or some other program to unlock the ISP's mailbox.

Pause server for xx seconds (-1 = infinite, 0=no waiting)
If the *Once Connected, Run This Process* control contains a valid entry then the server will pause its operations for the number of minutes specified here while it waits for the executing process to return. Entering "-1" will cause the server to wait indefinitely for the process to return.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Force process to shutdown after pause interval has elapsed
Sometimes the program you need to run may not exit once it has run its course; some programs require user intervention in order to close them down. This is not acceptable when the software must run unattended. If this switch is selected MDaemon will force the process thread to terminate once the number of seconds specified in *Pause Server For XX Seconds* has elapsed. This function does not work when the server is configured to wait indefinitely for the process to return.

3.1.4 LDAP/Address Book Settings

MDaemon supports Lightweight Directory Access Protocol (LDAP) functionality. Click "Setup » Server Settings » LDAP" to reach the LDAP screen used for configuring MDaemon to keep your LDAP server up to date on all of its user accounts. MDaemon can maintain an accurate and continuously up to date LDAP database of users by communicating with your LDAP server each time an MDaemon account is added or removed. This makes it possible for users with mail clients that support LDAP to "share" a global address book that will contain entries for all of your MDaemon users as well as any other contacts that you include.

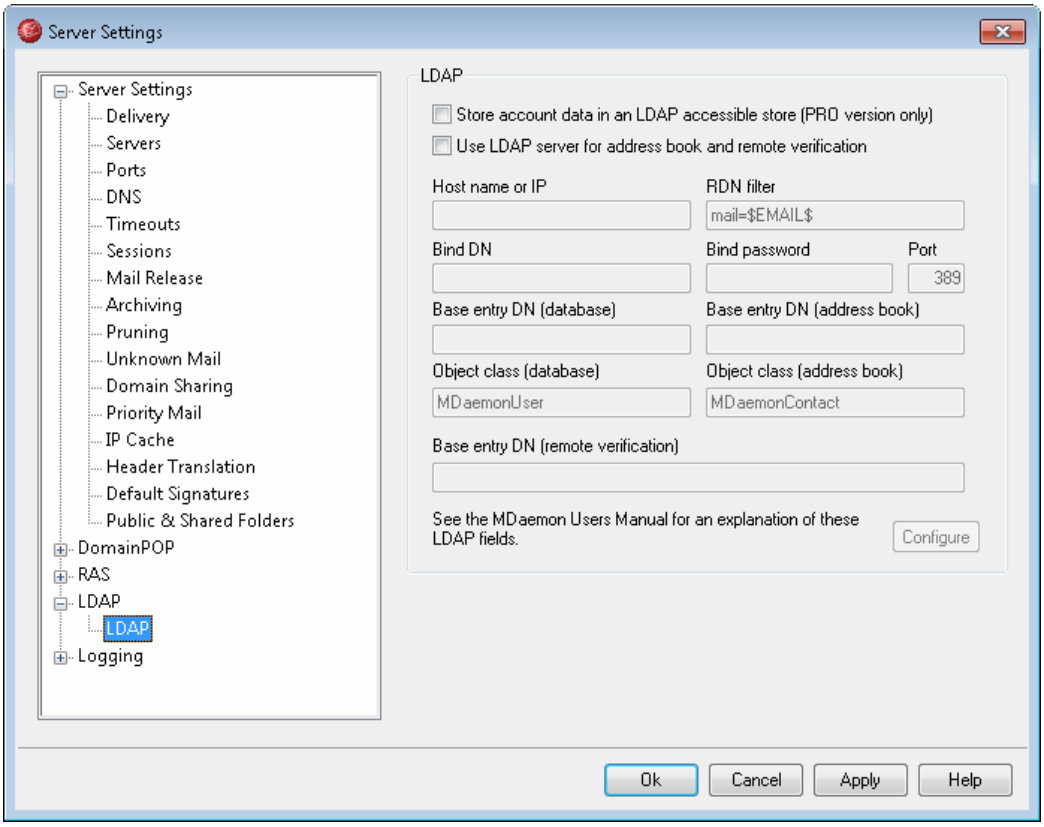
You can also use your LDAP server as the MDaemon user database rather than its local `USERLIST.DAT` system or an ODBC compliant database. You might want to use this method of maintaining your user information if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally.

See:

LDAP 106
Account Database Options 628

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.4.1 LDAP



LDAP

Store account data in an LDAP accessible store (PRO version only)
Click this check box if you want MDaemon to use your LDAP server as the MDaemon user database rather than ODBC or its local `USERLIST.DAT` system. You might want to use this method of maintaining your user information if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally.

Use LDAP server for address book and remote verification
If you are using ODBC or the default `USERLIST.DAT` method of maintaining your account database rather than the LDAP server method, you can still keep an LDAP server up to date with all of your users' names, email addresses, and aliases by enabling this checkbox. Thus, you can still keep an LDAP server up to date for use as a global address book system for users of email clients that contain support for LDAP address books.

This will maintain a database of your mailboxes, aliases, and mailing lists that your remote backup servers can query for remote verification of address information. See *Base entry DN (remote verification)* below for more information.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

LDAP Server Properties

Host name or IP
Enter the host name or IP address of your LDAP server here.

RDN filter
This control is used to generate the RDN for each user's LDAP entry. The relative distinguished name (RDN) is the leftmost component in each entry's distinguished name (DN). For all peer entries (those sharing a common immediate parent) the RDN must be unique, therefore we suggest using each user's email address as their RDN to avoid possible conflicts. Using the $EMAIL$ macro as the value of the attribute in this control (i.e. `mail=$EMAIL$`) will cause it to be replaced by the user's email address when their LDAP entry is created. The user's DN will be comprised of the RDN plus the *Base entry DN* below.

Bind DN
Enter the DN of the entry to which you have granted administrative access to your LDAP server so that MDaemon can add and modify your MDaemon user entries. This is the DN used for authentication in the bind operation.

Bind Password
This password will be passed to your LDAP server along with the *Bind DN* value for authentication.

Port
Specify the port that your LDAP server is monitoring. MDaemon will use this port when posting account information to it.

Base entry DN (database)
Enter the base entry (root DN) that will be used in all of your MDaemon user entries when you are using the LDAP server as your user database rather than the `USERLIST.DAT` file. The Base entry DN is combined with the RDN (see *RDN filter* above) to make up each user's distinguished name (DN).

Base entry DN (address book)
When mirroring account information to an LDAP database address book, enter the base entry (root DN) that will be used in all of your MDaemon user address book entries. The Base entry DN is combined with the RDN (see *RDN filter* above) to make up each user's distinguished name (DN).

Object class (database)
Specify the object class to which each MDaemon user's user database entry must belong. Each entry will contain the `objectclass=` attribute with this as its value.

Object class (address book)
Specify the object class to which each MDaemon user's LDAP address book entry must belong. Each entry will contain the `objectclass=` attribute with this as its value.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Base entry DN (remote verification)
One common problem with domain gateways and backup servers is that they don't usually have a method for determining whether or not the recipient of an incoming message is valid. For instance, if a message comes to example.com's backup server for `user1@example.com` then the backup server has no way of knowing whether or not there is actually a mailbox, alias, or mailing list at example.com for "`user1`". Thus the backup server has no choice but to accept all of the messages. MDaemon contains a method for verifying these addresses and solving this problem. By specifying a Base entry DN that will be used for all mailboxes, aliases, and mailing lists, your LDAP server can be kept up to date with all of this information. Then, your backup server can simply query your LDAP server each time a message arrives for your domain and verify whether or not the recipient's address is valid. If it isn't then the message will be rejected.

Configure
Click this button to open the `LDAP.dat` configuration file in a text editor. It is used for designating the LDAP attribute names that will correspond to each MDaemon account field.

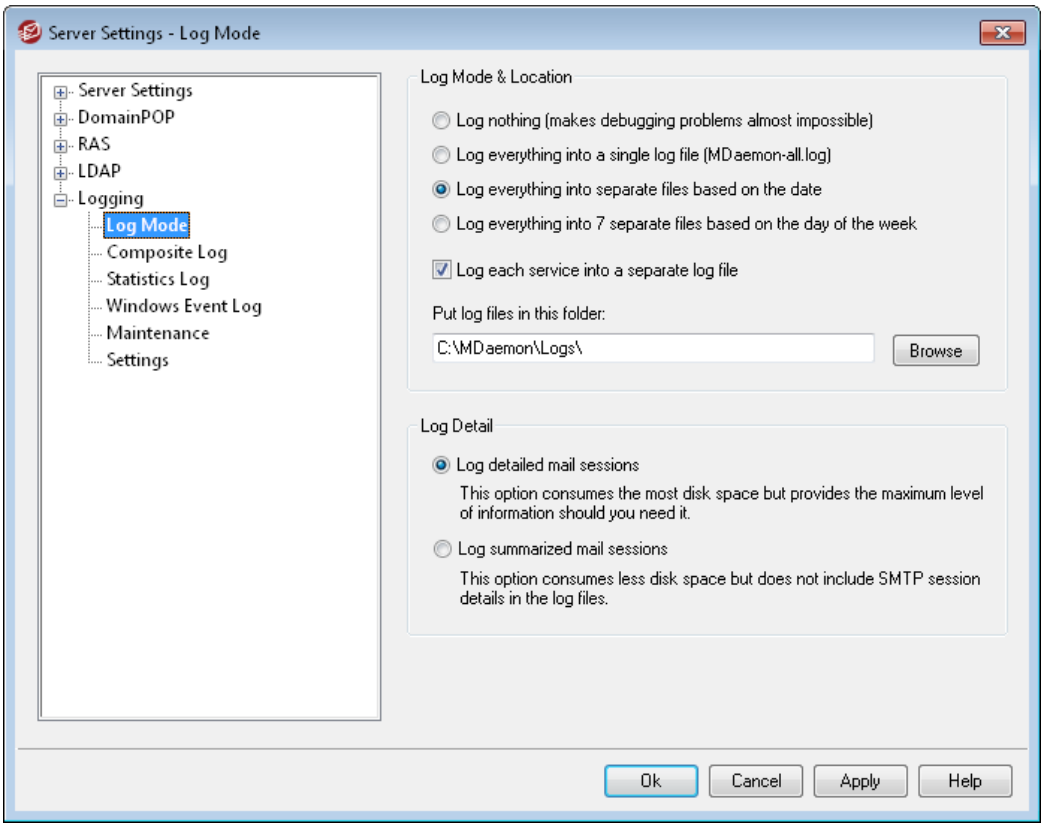
See:

Account Database Options 628

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.5 Logging

3.1.5.1 Log Mode


Server Settings - Log Mode
Server Settings
DomainPOP
RAS
LDAP
Logging
Log Mode
Composite Log
Statistics Log
Windows Event Log
Maintenance
Settings
Log Mode & Location
Log nothing (makes debugging problems almost impossible)
Log everything into a single log file (MDaemon-all.log)
Log everything into separate files based on the date
Log everything into 7 separate files based on the day of the week
Log each service into a separate log file
Put log files in this folder:
C:\MDaemon\Logs\
Browse
Log Detail
Log detailed mail sessions
This option consumes the most disk space but provides the maximum level of information should you need it.
Log summarized mail sessions
This option consumes less disk space but does not include SMTP session details in the log files.
Ok
Cancel
Apply
Help

Click the "Setup » Server Settings » Logging" menu selection to configure your logging settings. Logging is a useful tool for diagnosing problems and seeing what the server has been doing while unattended.

There are several options on the Preferences dialog governing the amount of log data that may be displayed in the Event Tracking pane of MDaemon's main interface. For more information, see Preferences » UI 344.

Log Mode & Location

Log nothing
Choosing this option will deactivate all logging. The log files will still be created, but no logging data will be written to them.

We do not recommend using this option. Without logs it can be extremely difficult, if not impossible, to diagnose or debug any potential email-related problems you may encounter.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Log everything into a separate log file (MDaemon-all.log)
Choose this option if you wish to log everything into a single, separate file named `MDaemon-all.log`.

Log everything into separate files based on the date
If this option is selected then a separate log file will be generated each day. The name of the file will correspond to the date it was created.

Log everything into 7 separate files based on the day of the week
If this option is selected, a separate log file will be generated for each day of the week. The name of the log file will correspond to the day of the week on which it was created.

Log each service into a separate log file
Click this checkbox to cause MDaemon to maintain separate logs by service rather than in a single file. For example, with this switch set MDaemon will log SMTP activity in the `MDaemon-SMTP.log` file and IMAP activity in the `MDaemon-IMAP.log` file. When running a Configuration Session or Terminal Services instance of the MDaemon interface, this option must be selected in order for the tabs on the interface to display the logged information.

Put log files in this folder:
Use this option if you wish to designate a specific folder path for your log files.

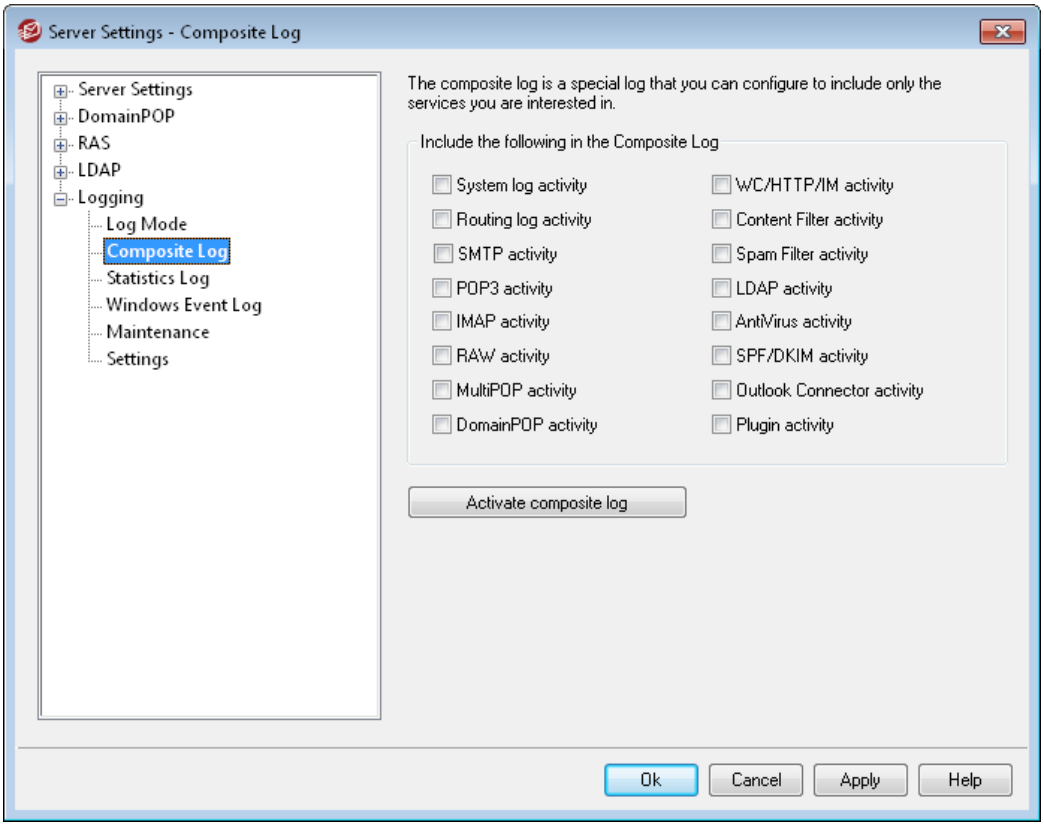
Log Detail

Log detailed mail sessions
A complete transcript of each mail transaction session will be copied to the log file when this option is active.

Log summarized mail sessions
The option causes a summarized transcript of each mail transaction session to be copied to the log file.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.5.2 Composite Log



Composite log

Include the following in the Composite Log
Located on the Windows menu of MDaemon's menu bar is a Composite Log View option. Clicking that option will add a window to MDaemon's main display that will combine the information displayed on one or more of the Event Tracker's tabs. Use the controls in this section to designate which tabs' information to combine in that window. The information contained on the following tabs can be combined:

System—Displays MDaemon's system activity such as initializing services and enabling/disabling any of MDaemon's various servers.

Routing—Displays the routing information (To, From, Message ID, and so on) for each message that is parsed by MDaemon.

SMTP—All send/receive session activity using the SMTP protocol is displayed.

POP3—When users collect email from MDaemon using the POP3 protocol, that activity is logged.

IMAP—Mail sessions using the IMAP protocol are logged.

RAW—RAW or system generated message activity is logged.

MultiPOP—Displays MDaemon's MultiPOP mail collection activities.

DomainPOP—Displays MDaemon's DomainPOP activity.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

WorldClient/HTTP/IM—Displays all WorldClient and instant messaging activity.

Content Filter—MDaemon's Content Filter operations are listed.

Spam Filter—Displays all Spam Filtering activity.

LDAP—Displays LDAP activity.

AntiVirus—AntiVirus operations are display in the composite view.

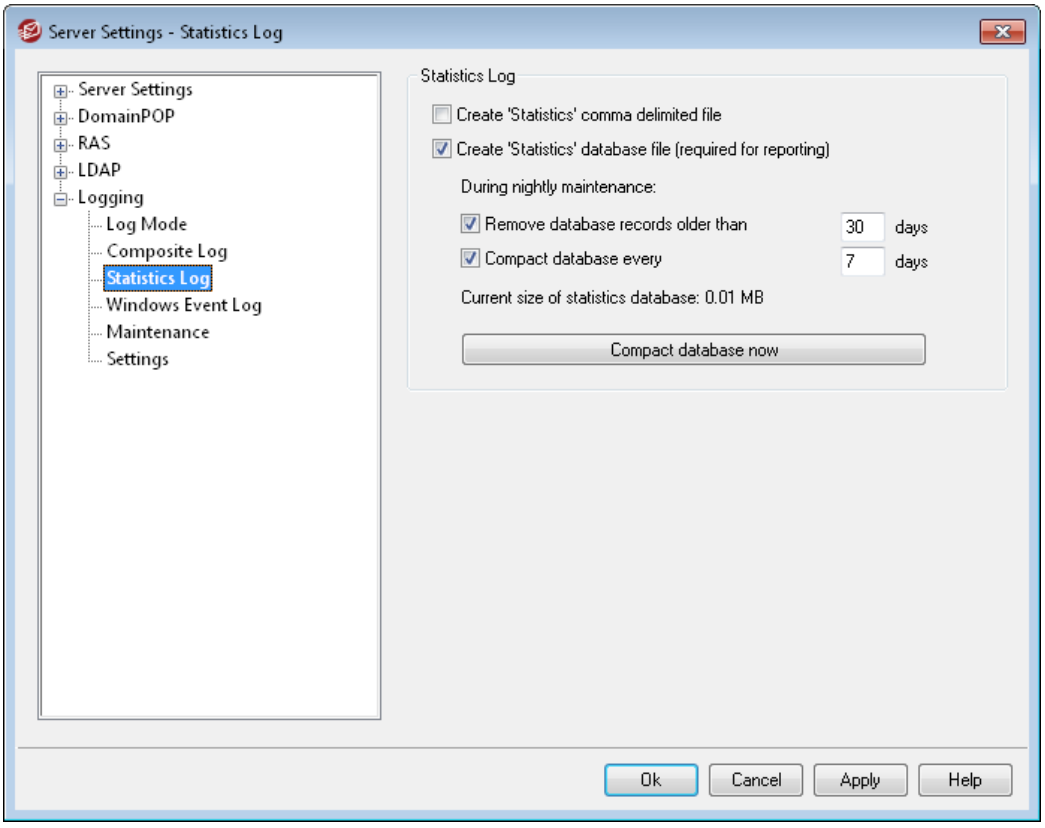
SPF/DKIM—Displays all Sender Policy Framework and DKIM activity.

Outlook Connector—Displays all Outlook Connector activity.

Plugin activity—Logs MDaemon plugin activities to the composite log.

Activate composite log
Click this button to launch the composite log window in MDaemon's main interface. It can also be activated from the Windows menu of MDaemon's menu bar.

3.1.5.3 Statistics Log



Statistics Log

Create 'Statistics' comma delimited file
Use this option if you wish to maintain a comma-delimited statistics file, containing

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

data on the number of inbound and outbound messages processed, spam statistics, antivirus statistics, and the like. This option is disabled by default.

Create 'Statistics' database file (required for reporting)
Check this box if you wish to log statistical information about MDaemon's activity to an SQLite database file. The database contains data on MDaemon's bandwidth usage, number of inbound and outbound messages, spam statistics, and the like. By default this database is stored in the "`MDaemon\StatsDB`" folder and 30 days worth of data are saved, but you can adjust how long to keep the data if you wish to retain more or less than the default 30 days. Data older than the designated limit will be removed during the nightly maintenance process. You can also specify how often MDaemon will compact the database to conserve space.

The Reports page in MDaemon's Remote Administration web interface uses this database to generate a variety of reports available to Global administrators. For each report, data may be generated for several predefined date ranges, or the admin may specify a custom date range. Administrators can choose from the following reports:

- Enhanced bandwidth reporting
- Inbound vs. Outbound messages
- Good messages vs. Junk messages (percentage of email that is spam or a virus)
- Inbound messages processed
- Top recipients by number of messages
- Top recipients by message size
- Outbound messages processed
- Top spam sources (domains)
- Top recipients of spam
- Viruses blocked, by time
- Viruses blocked, by name

During nightly maintenance:
The options below govern which database-related tasks MDaemon will perform during the nightly maintenance operation.

Remove database records older than [xx] days
Use this option to designate the number of days worth of statistical database records that you wish to keep. By default this option is enabled and set to 30 days.

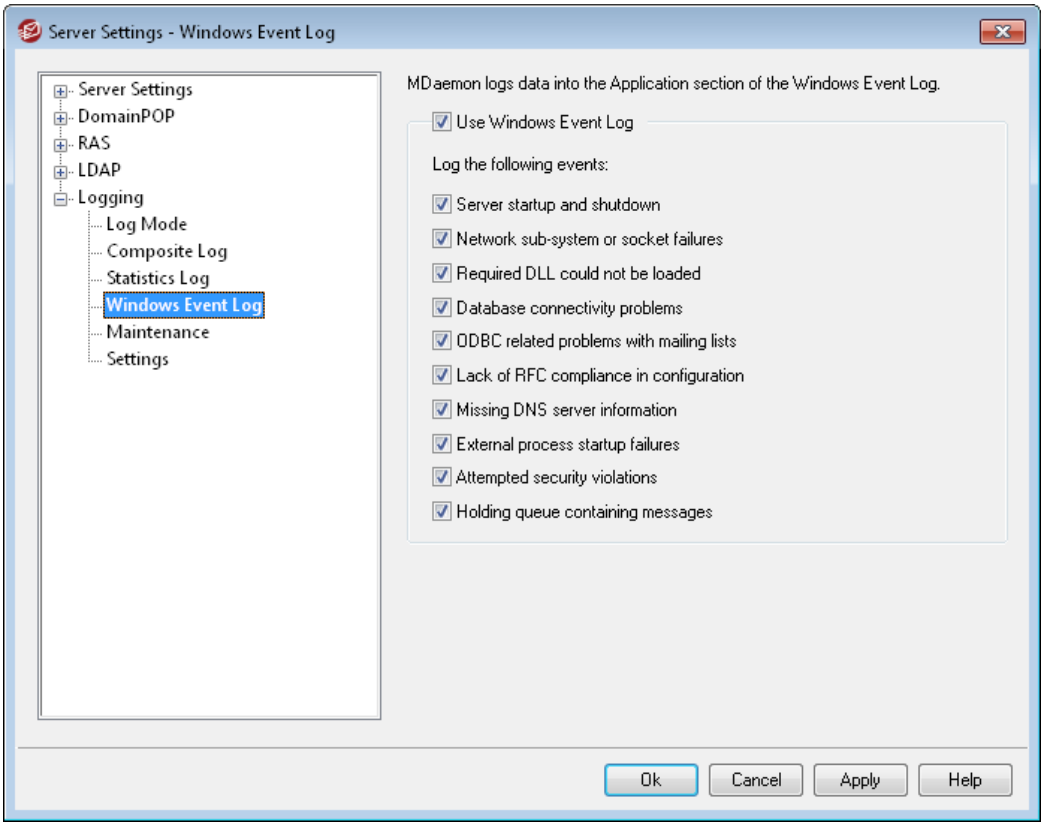
Compact database every [xx] days
Use this option if you wish to periodically compact the database to conserve space. By default this option is enabled and set to compact the database every 7 days.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Current size of statistics database:
The current size of your statistics database is listed here.

Compact database now
Click this button to immediately compact the database.

3.1.5.4 Windows Event Log

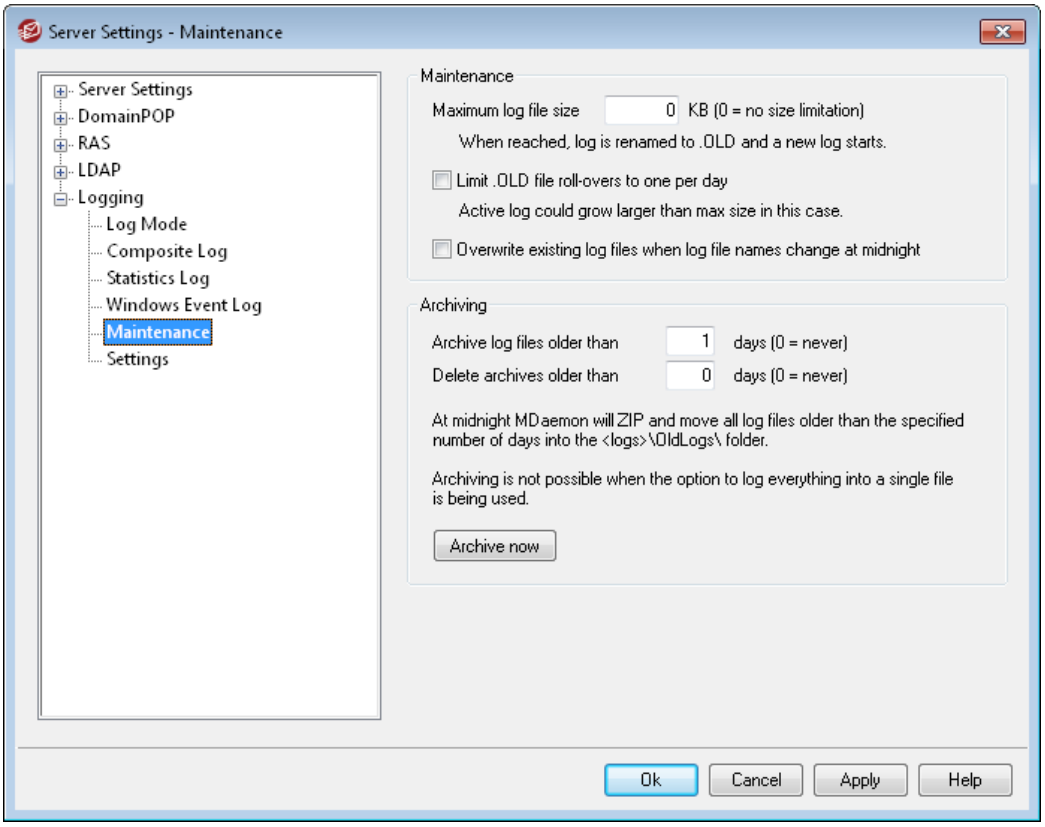


Use Windows Event Log
Click this check box if you want to log critical system errors, warnings, and certain other events into the Application section of the Windows Event Log.

Log the following events:
Use the options in this section to specify which events you wish to log.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.1.5.5 Maintenance


Server Settings - Maintenance
Server Settings
DomainPOP
RAS
LDAP
Logging
Log Mode
Composite Log
Statistics Log
Windows Event Log
Maintenance
Settings
Maintenance
Maximum log file size 0 KB (0 = no size limitation)
When reached, log is renamed to .OLD and a new log starts.
Limit .OLD file roll-overs to one per day
Active log could grow larger than max size in this case.
Overwrite existing log files when log file names change at midnight
Archiving
Archive log files older than 1 days (0 = never)
Delete archives older than 0 days (0 = never)
At midnight MDaemon will ZIP and move all log files older than the specified number of days into the <logs>\OldLogs\ folder.
Archiving is not possible when the option to log everything into a single file is being used.
Archive now
Ok
Cancel
Apply
Help

Maintenance

Maximum log file size [xx] KB
This is the maximum size in kilobytes that a log file may reach. Once this size is reached, the log file is `copied` to `LOGFILENAME.OLD` and a new log is started.

Limit .OLD file roll-overs to one per day
When limiting the log file size, click this checkbox if you want no more than one log file to be backed up per day. Each day, the first time that the maximum log file size is reached it will be renamed to "`*.OLD`" and saved normally. The subsequent log file will continue to grow regardless of the maximum size specified. It will not be rolled over until the next day — even if the maximum size setting is surpassed.

Overwrite existing log files when log file names change at midnight
By default, when MDaemon changes the log file's name at midnight and the filename to which it is changing already exists, it will append newly logged information to the existing file. For example, if MDaemon is changing from Monday.log to Tuesday.log and a file named Tuesday.log already exists, it will append newly logged data to the existing file rather than overwrite it or create a new one. Click this checkbox if you want MDaemon to overwrite any existing file rather than append new data to it.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

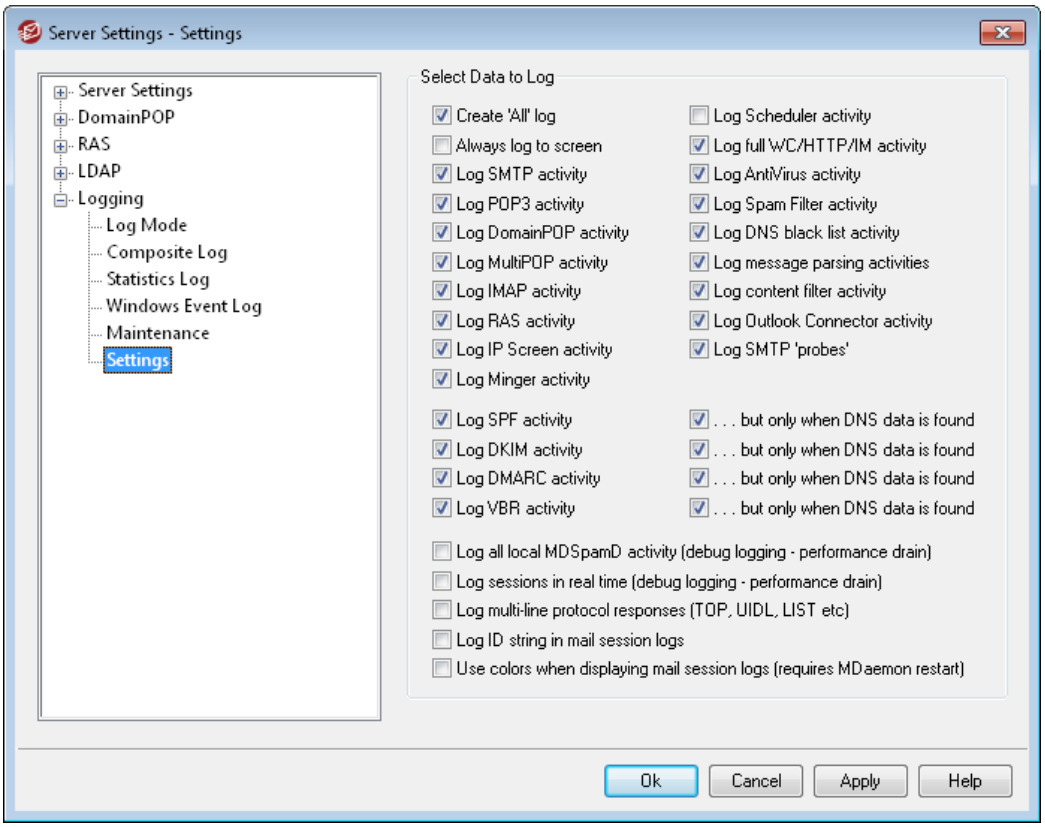
Archiving

Archive log files older than [XX] days (0=never)
Click this option if you want MDaemon to archive each log file whose age exceeds the number of days specified. Each day at midnight, MDaemon will `ZIP` old `*.log` and `*.old` files and move them to the `\Logs\OldLogs\` subfolder (deleting the original files in the process). This process will not archive or delete files that are in use, nor will it archive files when the "*Log everything into a separate log file (MDaemon-all.log)*" option is selected on the Log Mode 109 screen.

Delete archives older than [XX] days (0=never)
Use this option if you want MDaemon to delete archived log files automatically when their age exceeds the number of days specified here. Use "0" in this option if you do not wish to delete archives automatically. Archive deletion occurs during the daily midnight cleanup event.

Archive now
Click this button to archive old log files immediately rather than waiting for MDaemon to archive them automatically at midnight.

3.1.5.6 Settings



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Select Data to Log

Create 'All' log
Click this option if you want the "*-all.log" file to be generated, which contains a composite of all logged activities.

Always log to screen
Click this option if you want the logged data to be copied to the MDaemon GUI even when it is minimized or running in the tray.

When this control is cleared, log data isn't copied to the Event Tracking pane when MDaemon is running in the system tray. Consequently, the most recent activity won't be listed on any of the Event Tracking pane's tabs when MDaemon is first opened. It will begin displaying newly logged information from that point forward.

Log SMTP activity
Enable this option if you want to log all of MDaemon's send/receive SMTP activity.

Log POP3 activity
Click this checkbox to log all POP mail activity. This will log your users' POP mail collection sessions.

Log DomainPOP activity
Click this checkbox to log all DomainPOP mail activity.

Log MultiPOP activity
Click this checkbox to log all of your users' MultiPOP mail collection activity.

Log IMAP activity
Enabling this option causes all of your users' IMAP sessions to be included in MDaemon's log files.

Log RAS activity
Click this switch if you want MDaemon to copy RAS dialup/dialdown activities into the log file. This information is useful for diagnosing dialup problems.

Log IP Screen activity
Click this checkbox if you want the IP Screening activities to be included in MDaemon's log file.

Log Minger activity
Click this checkbox to log Minger server activities.

Log Scheduler activity
Enable this checkbox if you wish to log all of the Event Scheduler's 269 activity.

Log full WC/HTTP/IM activity
Click this option if you wish to log all WorldClient, HTTP, and WorldClient Instant Messenger activity. When disabled, WorldClient and HTTP logs will still be created showing WorldClient's startup and shutdown times, but other WC/HTTP/IM activity

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

will not be logged.

Log AntiVirus activity
This option logs SecurityPlus for MDaemon activities

Log Spam Filter activity
Logs all Spam Filter activity.

Log DNS black list activity
This option causes MDaemon to log DNS black list activity. Using this option will allow you to have an easy reference to the sites that were logged as blacklisted.

Log message parsing activities
MDaemon periodically performs a great deal of message parsing activity when determining to whom a message should be delivered. Enable this switch if you want this information to be included in the log file.

Log content filter activity
Click this checkbox if you want to include Content Filter activity in the log file.

Log Outlook Connector activity
This option governs whether or not Outlook Connector activities are logged.

Log SMTP 'probes'
Click this option to log SMTP sessions when no message data is transmitted by the sending server (i.e. the sending server does not use the DATA command).

Log SPF activity
Click this check box if you wish to log all Sender Policy Framework lookup activities.

> **...but only when DNS data is found**
> If you are logging SPF activities, click this check box if you wish to log only lookups where actual SPF data is found during the DNS lookup, rather than logging all SPF lookups.

Log DKIM activity
Click this option if you wish to log DomainKeys Identified Mail (DKIM) activity.

> **...but only when DNS data is found**
> Click this check box if you are logging DKIM activity but wish to log only those instances where DNS data is found instead of logging all activity.

Log DMARC activity
Click this option if you wish to log DMARC activity.

> **...but only when DNS data is found**
> Click this check box if you are logging DMARC activity but wish to log only those instances where DNS data is found instead of logging all activity.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Log VBR activity
Use this option if you wish to log message certification 469.

...but only when DNS data is found
If you are logging message certification activity, click this check box if you wish to log it only when actual certification data is found during the DNS lookup.

Log all local MDSpamD activity (debug logging—performance drain)
Use this option to log all local MDSpamD activities (see Caution below).

Log sessions in real time (debug logging—performance drain)
Ordinarily, session information is logged after the session is completed in order to conserve resources. Click this option if you want session information to be logged as it occurs.

When using either or both of the previous two logging options, you may see decreased performance in your mail system, depending on your system and the level of activity. Generally you should only use these options for debugging purposes.

Log multi-line protocol responses (like UIDL and LIST)
Sometimes the responses to protocol requests require more than one line of information. Click this checkbox if you want to log these additional lines.

Enabling this switch could potentially increase the amount of logged information a great deal. Because the number of lines in a response can't be determined in advance, and because some responses have great potential for "filling up" your log file with possibly unnecessary information (POP TOP, for example, lists the actual contents of the message), we do not recommend using this feature if log file size or verbosity is of concern to you.

Log ID string in mail session logs
Click this check box if you wish to include `[%d:%d]` ID strings in session logs.

Use colors when displaying mail session logs (requires MDaemon restart)
Enable this option if you wish to colorize the text displayed on several of the Event Tracking and Logging 41 tabs on MDaemon's user interface. This option is disabled by default, and enabling/disabling it requires an MDaemon restart before the change will take effect. See: "Colorized Session Logs" below for more information.

Colorized Session Logs

On MDaemon's user interface 41, the tabs that display Routing, SMTP-in, SMTP-out, IMAP, POP, MultiPOP, and DomainPOP activity can be colorized to help visually separate events during a session. This features is disabled by default, but can be enabled via the "*Use colors when displaying mail session logs*" option located at: Logging » Settings

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

116 and Preferences » UI 344. The default text colors can be changed by editing the `[Colors]` section of the `LogColors.dat` file. See the chart below for a list of the default colors.

If you want to use colors but don't want to colorize one or more of the listed elements, set value of each of those elements to zero (for example, `SpamFilter=0`). This will cause the chosen elements to use the `Default` color. For `Background` and `SelectedBackground`, however, setting their values to zero doesn't work. If you want to change either of those elements you will have to provide a new color value. Color values are specified in hexadecimal using this form: "`0xbbggrr`", where "bb" is the relative intensity for blue, "gg" for green, and "rr" for red. For example, "`Error=0x0000ff`" sets error text to red. **Please note:** this is the reverse of the traditional order for color codes, which is typically "`rrggbb`". If you make changes to the colors you must restart MDaemon or create of a file called `COLORS.SEM` and place it in MDaemon's `\APP\` folder.

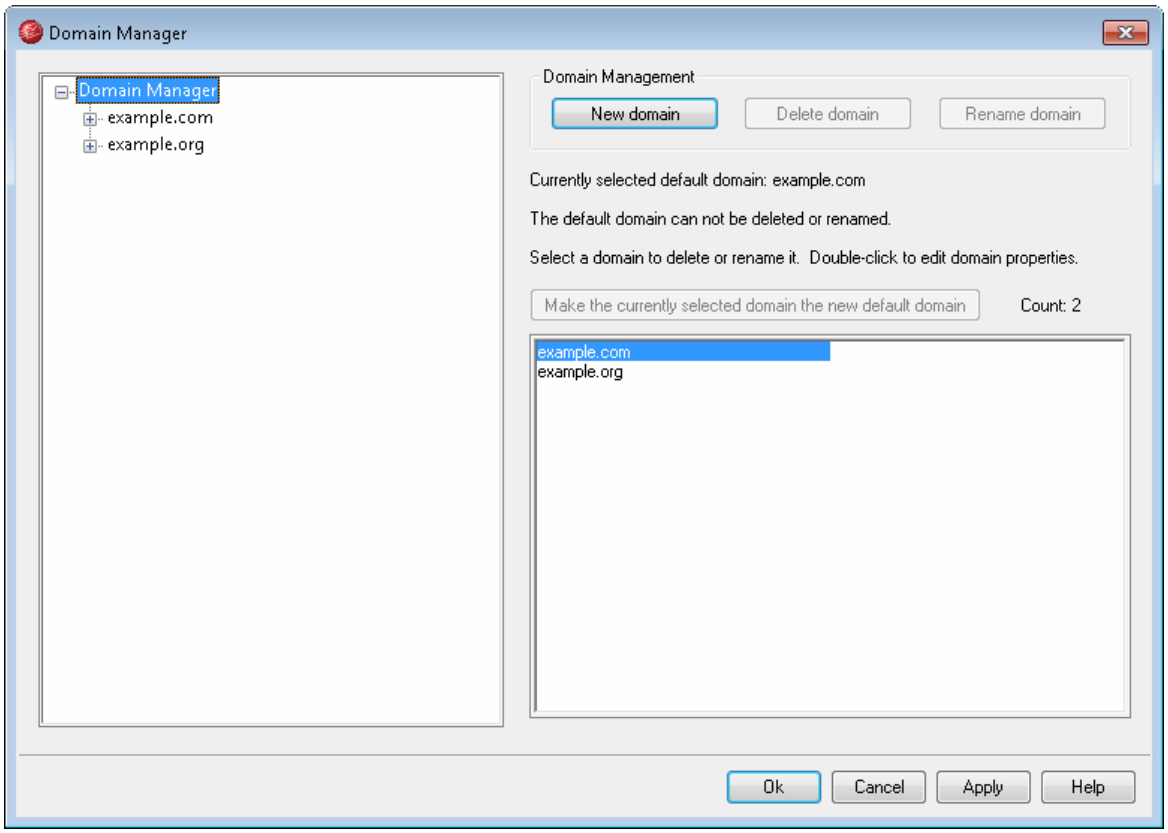
Default Log Colors

Background=0x000000	Background color; black
SelectedBackground=0xff0000	Selected background color; blue
Default=0xffffff	Default text color; white
Processing=0x00ffff	Internal processing and parsing activity; default is yellow
DataIn=0x008040	Incoming data from other server; default is dark green
DataOut=0x00ff00	Outgoing data sent to other server; default is bright green
Error=0x0000ff	Error messages; default is red
TCPIP=0xff8000	TCP/UDP/DNS/PTR related activity; default is light blue
SpamFilter=0x0080ff	Spam filtering; default is orange
AntiVirus=0xdda0dd	AntiVirus processing; default is plum
DKIM=0xff00ff	DKIM activity; default is fuchsia
VBR=0x40c0ff	Vouch by Reference activity; default is light orange
SPF=0x808080	Sender Policy Framework activity; default is grey
Plugins=0x0080c0	Any message sent from a plugin; default is brown
Localq=0x00ffff	Local queue routing; default is yellow
Spam=0x0080ff	Spam message routing; default is orange
Restricted=0x40c0ff	Restricted message routing; default is light orange

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

BlackList=0x808080	Blacklisted message routing; default is grey
Gateway=0x00ff00	Gateway message routing; default is light green
Inboundq=0xff8000	Inbound message routing; default is light blue
PublicFolder=0xdda0dd	Public folder message routing; default is plum

3.2 Domain Manager



MDaemon Pro contains full support for multiple domains, administered using the Domain Manager. Here you can manager the domain names, IP addresses, account and message pruning settings, WorldClient settings, and other domain-specific options for your domains.

MDaemon supports both single and multiple IP addresses, and IP addresses can be unique to individual domains or shared between them. Further, several key features such as Accounts, Mailing Lists, and some Security Settings are on a per domain basis. When you create an account, for example, you must specify the domain to which the new account belongs. The same goes for Mailing Lists. This also means that features such as the IP Screen 478 and IP Shield 440 are tied to domains individually.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Some features, such as Name Matching 99 under DomainPOP 88, are tied exclusively to the Default Domain. The Default Domain is also the domain displayed by default in various options, such as when creating new accounts or mailing lists. Further, to support MDaemon's handling of system messages, the following default Aliases 613 point several reserved mailbox names to MDaemon's default domain name rather than to its other domains:

```
MDaemon@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserver@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
list-serv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
```

Finally, in order to support multiple domains, by default MDaemon requires users to use their full email address (e.g. "user01@example.com") as their login value rather than using just the mailbox portion of the address (i.e. "user01"). Some very old mail clients, however, do not support using '@' in the login field. Therefore to accommodate those clients you can specify an alternate character on the System 347 screen under Preferences. Further, this value can be up to 10 characters long, making it possible to provide a string of characters to serve as the delimiter instead of only a single character such as '$'. For example, using '**.at.**' will allow you to make logon values of "user02.at.example.com". You can also disable the full email address requirement, allowing the use of only the mailbox portion of the address as the login value, but that is not recommended and can cause problems when you have more than one domain.

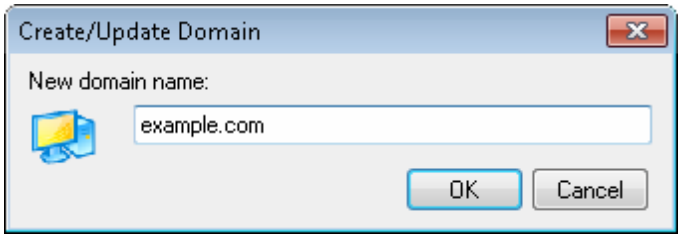
Domains List

The area on the left side of this dialog contains the list of your domains, with links to each screen used for configuring the various domain-specific settings. The Default Domain is listed first and all other domains are listed alphabetically. The list on the right is used for deleting and renaming domains, and for designating the Default Domain. You can double-click a domain in this list to switch to the domain and configure its settings.

Domain Management

New domain

To create a new domain: click *New domain*, enter the domain name in the Create/ Update Domain dialog, and click *OK*.



Typically the value entered here will be the registered Internet domain name that a DNS server resolves to the IP address of the local machine running the server, or a qualified alias of that name. Alternatively, you may choose to use an internal-only or otherwise non-valid, non-public domain name (such as "company.mail") for your domain name. When configuring your server in this way it may be necessary to use the Header Translation 81 feature, and/or the Domain Name Replacement Engine 95,

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

to enable proper mail distribution.

Delete domain
To delete a domain: select the domain from the list below, click *Delete domain*, and then confirm your decision to delete the domain by clicking *Yes*.

You cannot delete or rename the default domain. If you wish to delete or rename it then you must first designate a different domain as the default domain.

Rename domain
To change a domain name: select a domain from the list below, click *Rename domain*, type the new domain name in the Create/Update Domain dialog, and click *OK*.

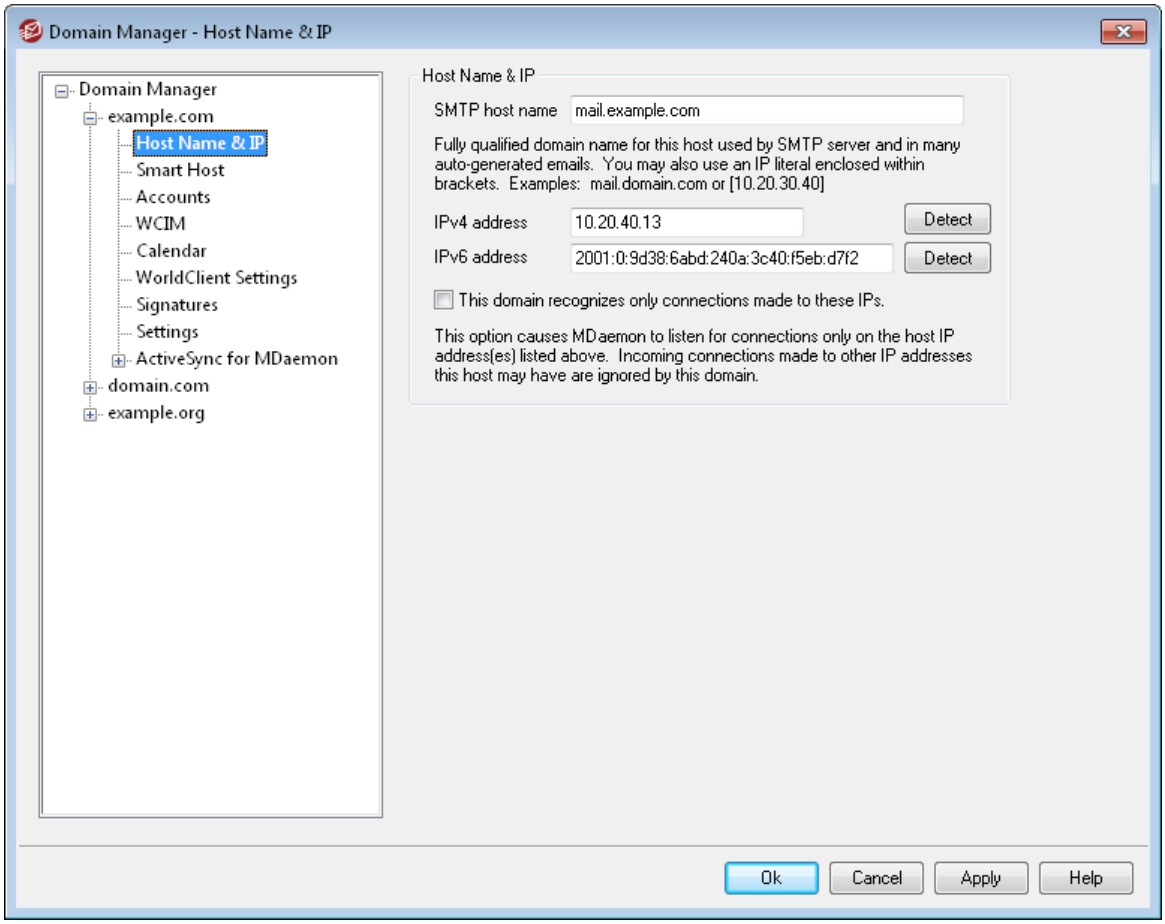
Make the currently selected domain the new default domain
If you wish to change MDaemon's default domain, selected the desired domain from the list below and click this button.

See:

Preferences » System 347

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.2.1 Host Name & IP


Domain Manager - Host Name & IP
Domain Manager
example.com
Host Name & IP
Smart Host
Accounts
WCIM
Calendar
WorldClient Settings
Signatures
Settings
ActiveSync for MDaemon
domain.com
example.org
Host Name & IP
SMTP host name
mail.example.com
Fully qualified domain name for this host used by SMTP server and in many auto-generated emails. You may also use an IP literal enclosed within brackets. Examples: mail.domain.com or [10.20.30.40]
IPv4 address
10.20.40.13
Detect
IPv6 address
2001:0:9d38:6abd:240a:3c40:f5eb:d7f2
Detect
This domain recognizes only connections made to these IPs.
This option causes MDaemon to listen for connections only on the host IP address(es) listed above. Incoming connections made to other IP addresses this host may have are ignored by this domain.
Ok
Cancel
Apply
Help

Host Name & IP

SMTP host name
This value is the Fully Qualified Domain Name (FQDN) that will be used in the `SMTP HELO/EHLO` instruction when sending mail for this domain. For incoming connections, if the *This domain recognizes only connections made to the host IP address* option below is used, the domain is bound to its own IP address and the proper FQDN will be used for connections made to that domain. Using that option, however, is not strictly required for this to work. But, if you have two or more domains using the same unbound IP address then the FQDN used will be the one that is associated with the domain that is first in alphabetical order.

In most cases the FQDN will be either the *Domain name* or a subdomain of it (for example, "`mail.example.com`"), but an IP literal syntax such as "`[192.0.2.0]`" may also be used. When no FQDN value is specified, MDaemon will use the Default Domain's FQDN.

IPv4/IPv6 address
Enter the IPv4 and IPv6 addresses to associate with this domain. If an IP address is missing MDaemon will automatically try to detect a suitable address for use.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

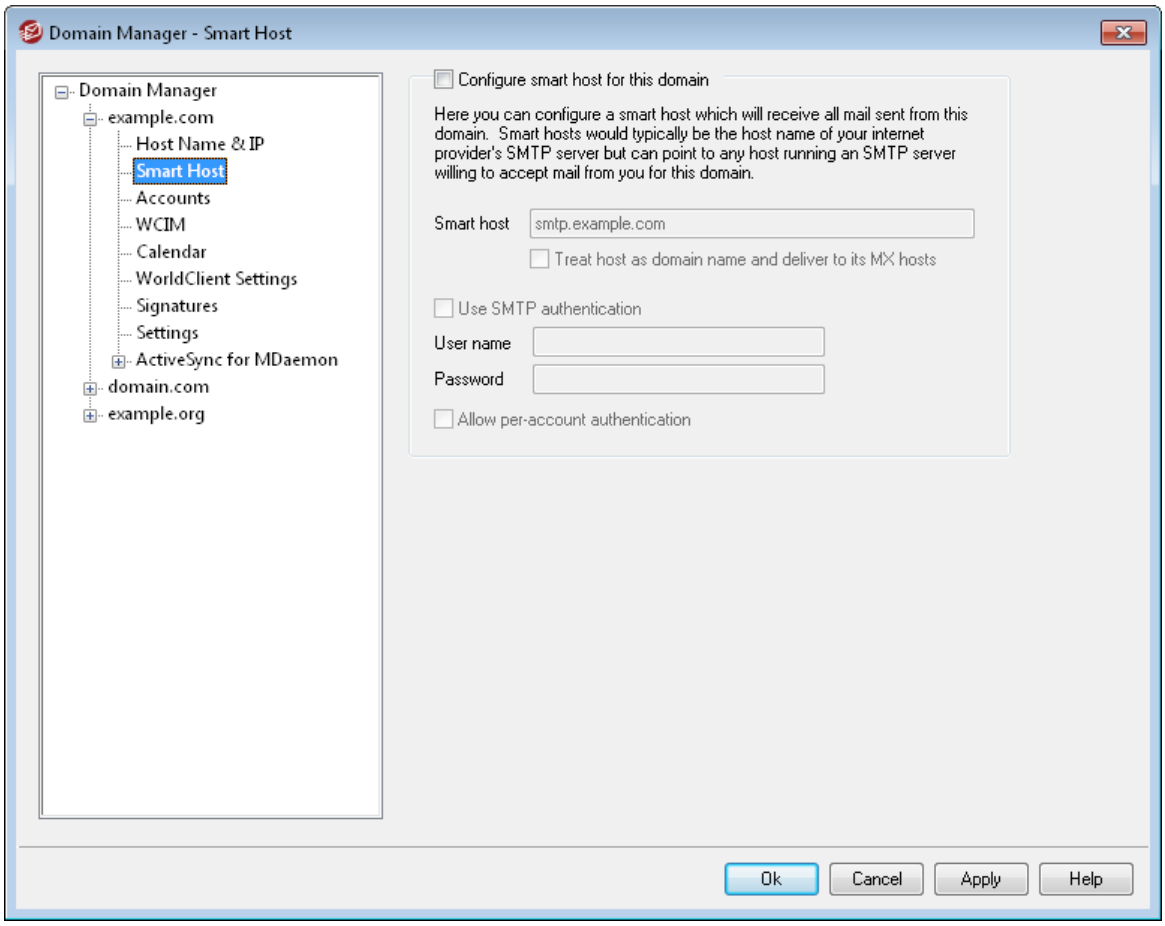
Detect
Use these buttons to detect the IPv4 and IPv6 IP addresses that are eligible for use in the corresponding IP address options. You can then choose from the IP addresses listed.

This domain recognizes only connections made to these IPs
Click this checkbox if you wish to restrict this domain's incoming connections to the IP addresses specified above. By default this only applies to inbound connections. Outbound socket binding is governed by an option under "Server Settings » Binding 61."

See:

Domain Manager 121
Preferences » System 347
Binding 61
IPv6 60

3.2.2 Smart Host


Domain Manager - Smart Host
Domain Manager
example.com
Host Name & IP
Smart Host
Accounts
WCIM
Calendar
WorldClient Settings
Signatures
Settings
ActiveSync for MDaemon
domain.com
example.org
Configure smart host for this domain
Here you can configure a smart host which will receive all mail sent from this domain. Smart hosts would typically be the host name of your internet provider's SMTP server but can point to any host running an SMTP server willing to accept mail from you for this domain.
Smart host
smtp.example.com
Treat host as domain name and deliver to its MX hosts
Use SMTP authentication
User name
Password
Allow per-account authentication
Ok
Cancel
Apply
Help

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Configure smart host for this domain

If you wish to route this domain's outbound mail through a specific Smart Host rather than using MDaemon's default Delivery 501 options, enable this checkbox and specify the smart host below. All of the domain's outbound mail will be routed to the host.

Smart host
Specify your ISP or mail host's name or IP address here. This is generally the SMTP server of your ISP.

Do not enter MDaemon's Default Domain or IP addresses into this text box. This entry should be an ISP or other mail server that can relay mail for you.

Treat host as domain name and deliver to its MX hosts
Check this box if you wish to treat the host as a domain name rather than a specific server, thus causing MDaemon to retrieve any MX hosts associated with the domain and connect to them.

Use SMTP authentication
Click this check box and enter your login credentials below if the *Smart Host* requires authentication. These login credentials will be used for all outbound SMTP messages sent to the smart host. If, however, you choose to use the *Allow per-account authentication* option below, then MDaemon will authenticate to the host separately for each message, using the sending account's *Smart Host Access* credentials designated on the Mail Services 525 screen of the Account Editor.

User name
Enter your user name or login here.

Password
Use this option to specify your smart host login password.

Allow per-account authentication
Click this checkbox if you wish to use per-account authentication for outbound SMTP messages sent to the *Smart Host* specified above. Instead of using the *User name* and *Password* credentials provided here, each account's *Smart Host Access* credentials, designated on the Mail Services 525 screen, will be used instead. If no smart host credentials have been designated for a given account, the above credentials will be used instead.

If you wish to configure *per-account authentication* to use each account's *Email password* instead of its optional *Smart host password*, then you can do so by editing the following key in the `MDaemon.ini` file:

```
[AUTH]
ISPAUTHUsePasswords=Yes (default No)
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

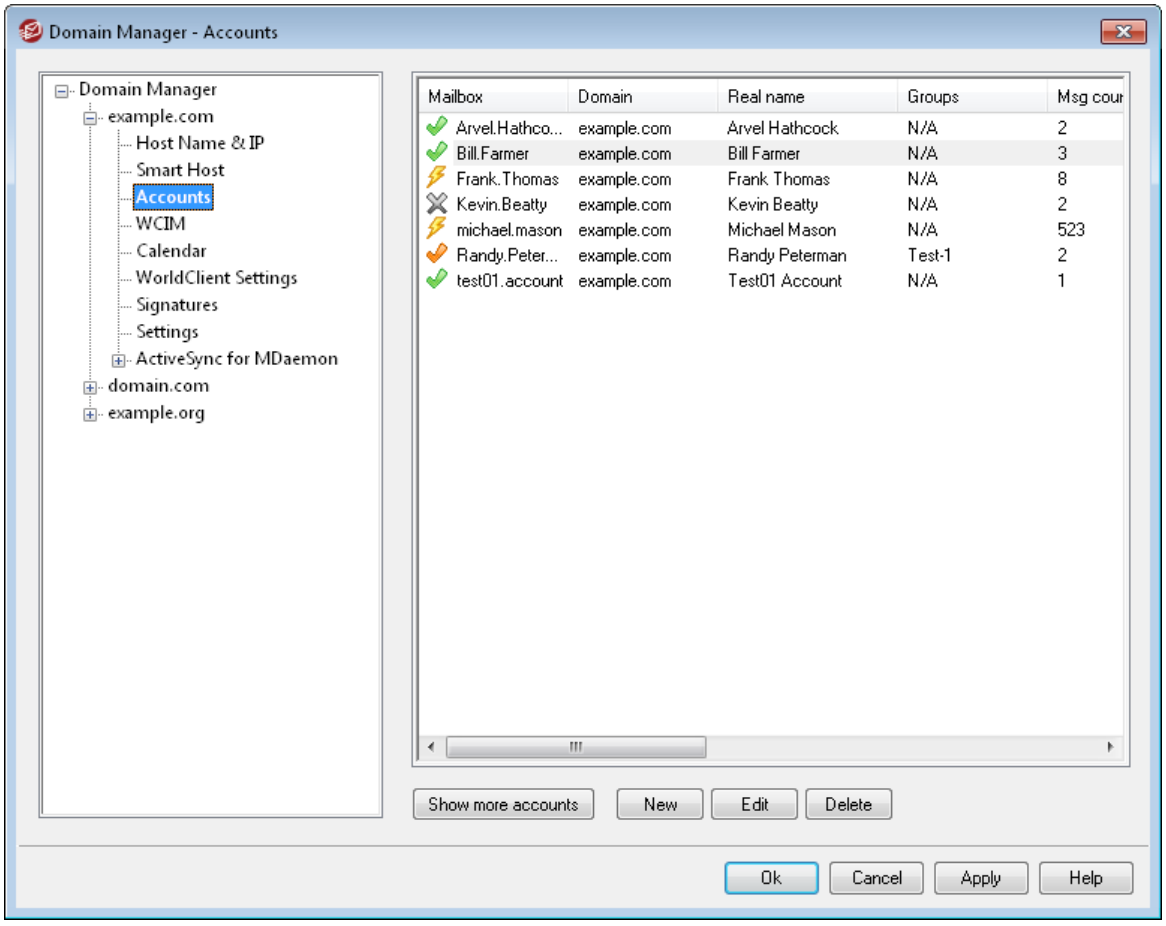
Enabling the `ISPAUTHUsePasswords=Yes` option will over time effectively communicate all your accounts' local mail passwords to your smart host. This could pose a risk to mail security, since it is providing sensitive information to another server. You should not use this option unless you are using a smart host that you absolutely trust and you believe it is necessary to do so. Further, you should note that if you use this option and give your users permission to change their *Email password* via WorldClient or some other means, then changing the *Email password* will also effectively change the *Smart host password*. This could cause smart host authentication to fail for an account when its *Email password* is changed locally but the corresponding *Smart host password* isn't changed at your smart host.

See:

Domain Manager 121
Server Settings » Delivery 50
Account Editor » Mail Services 525

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.2.3 Accounts



The Accounts page displays a list of all of this domain's MDaemon accounts. Each entry in the list contains Account Status Icons (see below), the mailbox, the "real name" of the account holder, any groups to which the account belongs, the message count, and the amount of disk space used (in MB). This list can be sorted in ascending and descending order by whichever column that you prefer. Click any column heading to sort the list in ascending order by that column. Click the column again to sort it in descending order.

Account Status Icons

Account is a global or domain administrator.

Full access account. Both POP and IMAP access are enabled.

Restricted access account. Either POP, IMAP, or both are disabled.

Account is frozen. MDaemon will still accept mail for the account, but the user cannot send or

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

check mail.

Disabled account. All access to the account is disabled.

New
Click this button to open the Account Editor[521] in order to create a new account.

Edit
Select an account from the list and then click this button to open it in the Account Editor[521]. You can also double-click the account to open it.

Delete
Select an account from the list and then click this button to delete it. You will be asked to confirm your decision to delete the account before MDaemon will proceed.

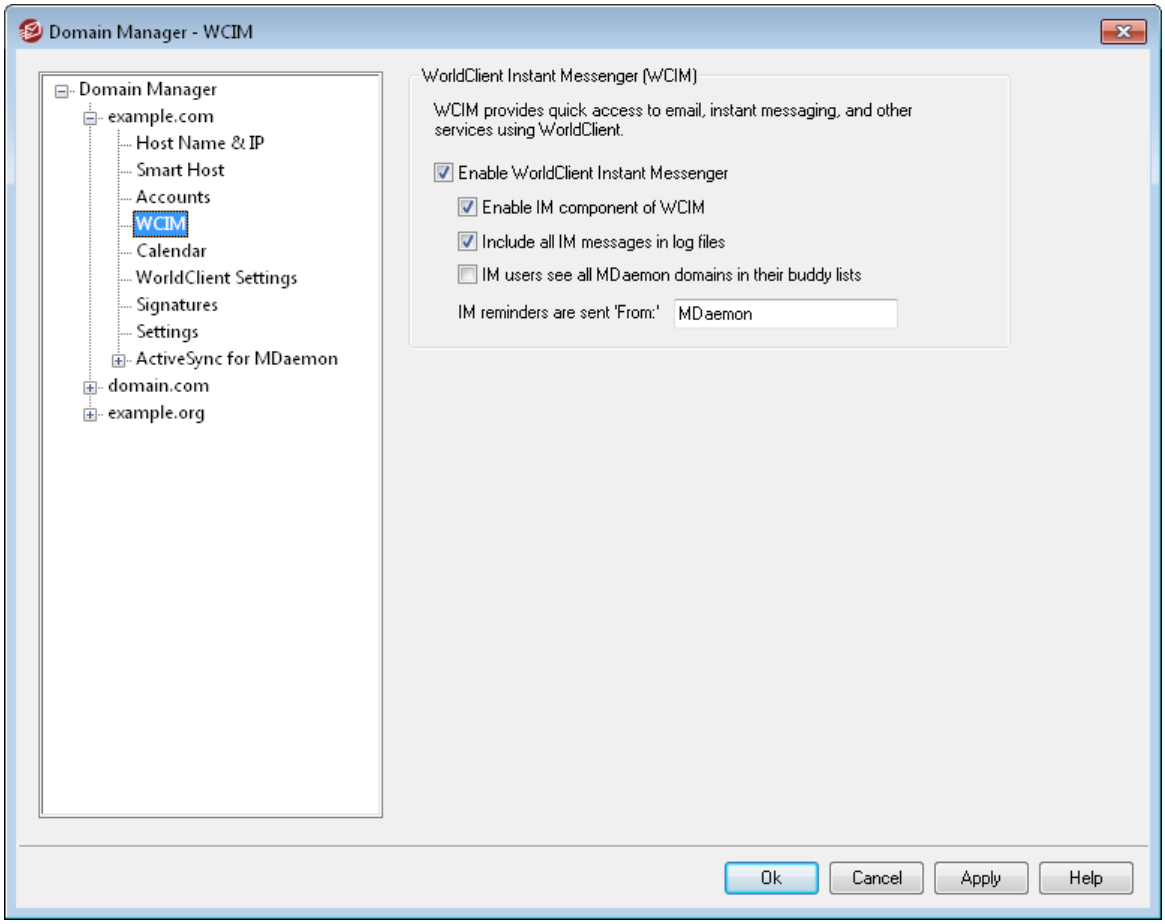
Show more accounts
The account list will only display 500 accounts at a time. If there are more than 500 accounts in the domain that you have chosen then click this button to display the next 500.

See:

Account Manager[518]
Account Editor[521]
New Accounts Template[581]

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.2.4 WCIM



This screen controls various aspects of WorldClient Instant Messenger (WCIM) 225 for this domain. The initial settings on this screen are determined by the Default WorldClient Instant Messenger 239 settings located on the Web & IM Services dialog. WCIM services can be enabled or disabled for specific accounts or groups via the Web Services 526 and Group Properties 577 screens respectively.

WorldClient Instant Messenger (WCIM)

Enable WorldClient Instant Messenger
This option makes WorldClient Instant Messenger available to the domain's users. They can download it from the Options » WorldClient Instant Messenger page within WorldClient. The downloaded installation file will be automatically customized for each user's account to make installation and setup easier.

Enable IM component of WCIM
Click this option if you want to activate WCIM's instant messaging (IM) system for the domain's users. Clear the check box if you want the IM controls to be unavailable.

Include all IM messages in log files
Click this check box if you want all of the domain's instant messaging traffic to be

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

included in the `InstantMessaging.log` file (located in the `MDaemon/LOGS/` folder).

IM users see all MDaemon domains in their buddy lists
Click this option if you want all of your MDaemon users (regardless of the domain) to be available for adding to this domain's buddy lists. Clear this checkbox if you want only users of this domain to be available for adding to buddy lists. For example, if your MDaemon is hosting mail for example.com and example.org, then activating this control for your example.com users will enable them to add buddies to their lists from both domains. Clearing it would mean that they could only add other example.com users.

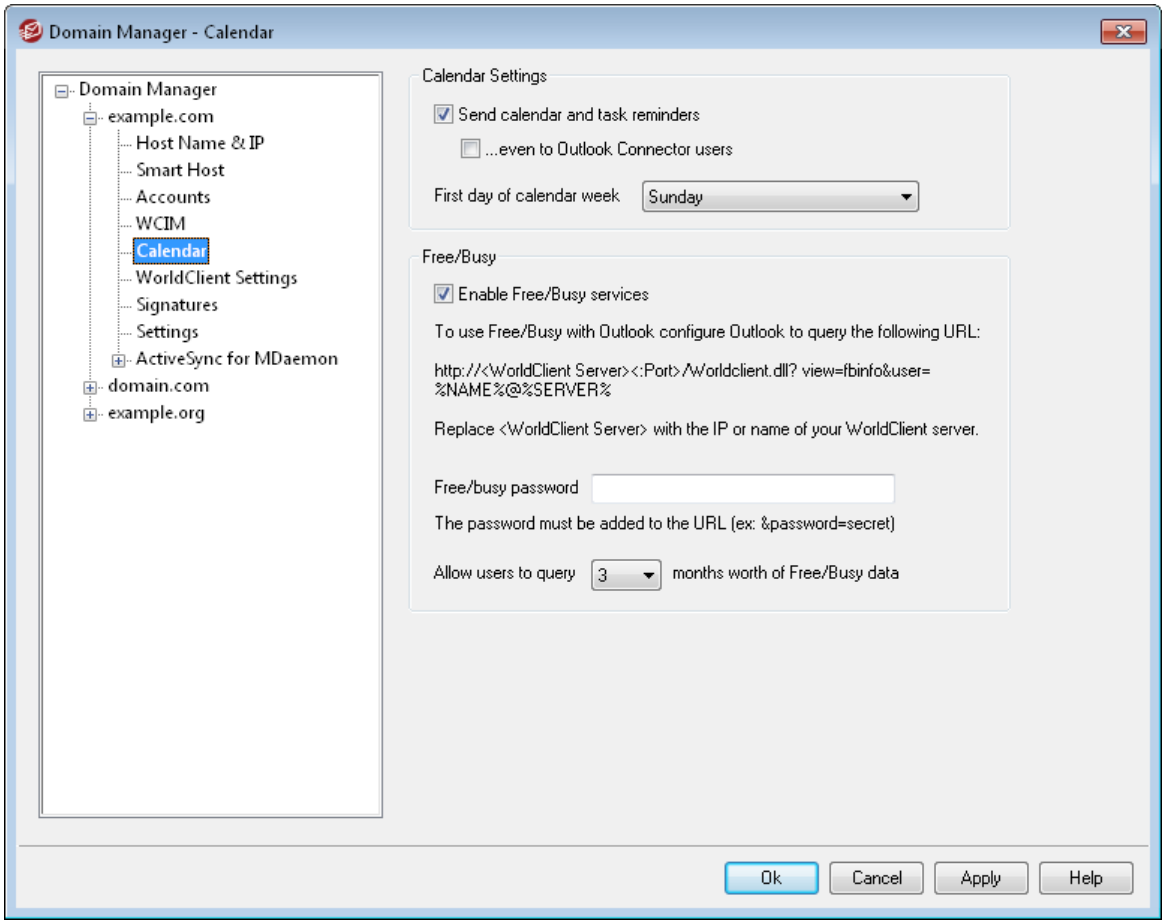
IM reminders are sent 'From:' [*text*]
When an appointment is scheduled on a user's WorldClient calendar, the event can be set to send a reminder to the user at a specified time. If the IM system is active for the user's domain then the reminder will be sent in an instant message if he or she is using WorldClient Instant Messenger. Use this text box to specify the name that you wish the message to appear to be 'From:'.

See:

Domain Manager 121
WorldClient (web mail) » WCIM 239
Account Editor » Web Services 526
Group Properties 577

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.2.5 Calendar



This screen controls MDaemon's Calendar features for this domain. The initial settings on this screen are determined by the Calendar 241 screen located on the Web & IM Services dialog.

Calendar Settings

Send calendar and task reminders
Click this checkbox if you wish to allow WorldClient's calendar and task reminders to be sent to your users via email and WorldClient Instant Messenger.

...even to Outlook Connector users
If you have enabled the "*Send calendar and task reminders*" option above, click this option if you also wish to enable reminders for Outlook Connector users.

First day of week
Choose a day from the drop-down list. The selected day will appear in the calendars as the first day of the week.

Free/Busy

MDaemon includes a Free/Busy server, which makes it possible for a meeting planner

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

to view the availability of potential meeting attendees. To access this feature, click Scheduling within WorldClient when creating a new appointment. This opens a Scheduling window containing the list of attendees and a color-coded calendar grid with a row for each one. Each attendee's row is color-coded to indicate the times at which he or she might be available for a meeting. There are colors for Busy, Tentative, Out of Office, and No information. There is also an Auto-Pick Next button that makes it possible for you to query the server for the next time slot at which all attendees may be available. When you have finished creating the appointment it will send an invitation to all of the attendees, who can then accept or decline.

WorldClient's Free/Busy server is also compatible with Microsoft Outlook. To use it, configure Outlook to query the URL listed below for Free/Busy data. In Outlook 2002, for example, the Free/Busy options are located under "Tools » Options » Calendar Options... » Free/Busy Options..."

Free/Busy server URL for Outlook:

```
http://<WorldClient><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%
@%SERVER%
```

Replace "<WorldClient>" with the IP address or domain name of your WorldClient server, and "<:Port>" with the port number (if you aren't using the default web port). For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

For more on how to use WorldClient's Free/Busy features to schedule your appointments, see the online Help system within WorldClient.

Enable Free/Busy services
Click this option if you wish to provide access to the Free/Busy server features to users.

Free/Busy password
If you wish to require a password when users attempt to access the Free/Busy server features via Outlook, include the password here. This password must be appended to the URL listed above (in the form: "&password=FBServerPass") when the users configure their Free/Busy settings within Outlook. For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%&password=MyFBServerPassword
```

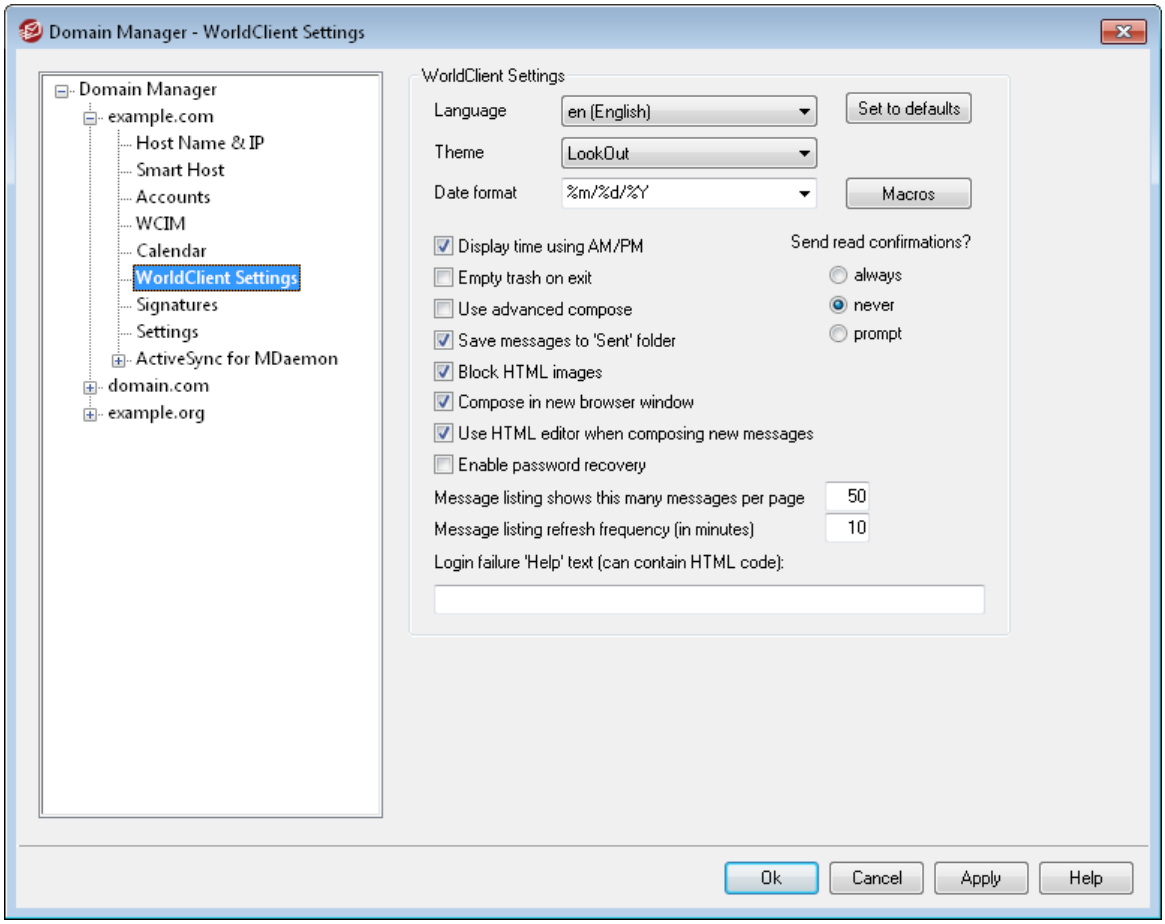
Allow users to query X months worth of Free/Busy data
Use this option to designate how many months worth of Free/Busy data your users may query.

See:

WorldClient (web mail) » Calendar 241

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.2.6 WorldClient Settings



This screen governs various WorldClient client-level options for this domain. When a user signs in to WorldClient, these options govern how WorldClient initially works for that user. Many of these settings can then be customized by the user via the Options pages within WorldClient. The default settings of this screen are determined by the WorldClient (web mail) » Settings 247 screen located on the Web & IM Services dialog.

WorldClient Settings

Set to defaults
This button resets a domain to the Default WorldClient Settings 247.

Language
Use the drop-down list box to choose the default language in which the WorldClient interface will appear when your users first sign in to the selected domain. Users can change their personal language setting on the WorldClient Sign-in page, and through an option in Options » Personalize within WorldClient.

Theme
Use this drop-down list box to designate the default WorldClient theme to use for the selected domain's users whenever they sign in for the first time. The users can

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

personalize the theme setting from Options » Personalize within WorldClient.

Date format
Use this text box to designate how dates will be formatted for the selected domain. Click the *Macros* button to display a list of macro codes that can be used in this text box. You can use the following macros in this control:

%A — Full weekday name

%B — Full month name

%d — Day of month (displays as "01-31")

%m — Month (displays as "01-12")

%y — 2-digit year

%Y — 4-digit year

For example, "`%m/%d/%Y`" might be displayed in WorldClient as "`12/25/2011`".

Macros
Click this button to display the list of macro codes that can be used in the *Date format*.

Display time using AM/PM
Click this option if you want a 12-hour clock with AM/PM to be used within WorldClient for times displayed for this domain. Clear the check box if you want to use a 24-hour clock for the domain. Individual users can modify this setting via the "*Display my hours in an AM/PM format*" option located on the Options » Calendar page within WorldClient.

Empty trash on exit
This option causes the user's trash to be emptied when he or she signs out from WorldClient. Individual users can modify this setting from the Options » Personalize page within WorldClient.

Use advanced compose
Check this box if you wish the domain's users to see the Advanced Compose screen in WorldClient rather than the normal Compose screen by default. Individual users can modify this setting from Options » Compose within WorldClient.

Save messages to 'Sent' folder
Click this option if you want a copy of each message that you send to be saved in your mailbox's *Sent* folder. Individual users can modify this setting from the Options » Compose page within WorldClient.

Block HTML images
Enable this check box if you wish to prevent remote images from being displayed automatically when viewing HTML email messages in WorldClient. In order to view the images the user must click the bar that appears above the message in the browser window. This is a spam prevention feature, because many spam messages

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

contain images with special URLs that identify the email address of the user who viewed the images, thus confirming to the spammer that it is a valid, working address. This option is enabled by default.

Compose in new browser window
Check this box if you want a separate browser window to open for composing messages instead of simply switching the main window to the compose screen. Clear the box if you do not want separate windows to open. Individual users can modify this setting from the Options » Compose page within WorldClient.

Use HTML editor when composing new messages
Check this box if you want the domain's users to see the HTML compose editor by default in WorldClient. They can control this setting for themselves from Options » Compose within **WorldClient**.

Enable password recovery
If enabled, domain users who have permission to edit their password 526 will be able to enter an alternate email address in WorldClient, which can be sent a link to reset their password if they forget it. To set up this feature, users must enter both the password recovery email address and their current password in WorldClient on the Options » Personalize page. Once set, if the user attempts to log in to WorldClient with an incorrect password a "forgot password?" link will appear. This link takes them to a page that asks them to confirm their password recovery email address. If entered correctly, an email will be sent with a link to a change password page. This feature is disabled by default.

You can enable or disable this option on a per-user basis by adding the following key to a WorldClient user's `user.ini` file (e.g. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (or "=No" to disable the option for the user)
```

Send read confirmations?
This option governs how WorldClient will respond to incoming messages that contain a request for read confirmation.

always
If this option is selected, MDaemon will send a notification to the sender indicating that the message was read. The WorldClient user who received the message will not see any indication that the read confirmation was requested or responded to.

never
Choose this option if you want WorldClient to ignore read confirmation requests.

prompt
Select this option if you wish to ask WorldClient users whether or not to send a read confirmation each time a message is opened that requests it.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Message listing shows this many messages per page
This is the number of messages that will be listed on each page of the Message Listing for each of your mail folders. If a folder contains more than this number of messages then there will be controls above and below the listing that will allow you to move to the other pages. Individual users can modify this setting from Options » Personalize within WorldClient.

Message listing refresh frequency (in minutes)
This is the number of minutes that WorldClient will wait before automatically refreshing the Message Listing. Individual users can modify this setting from Options » Personalize within WorldClient.

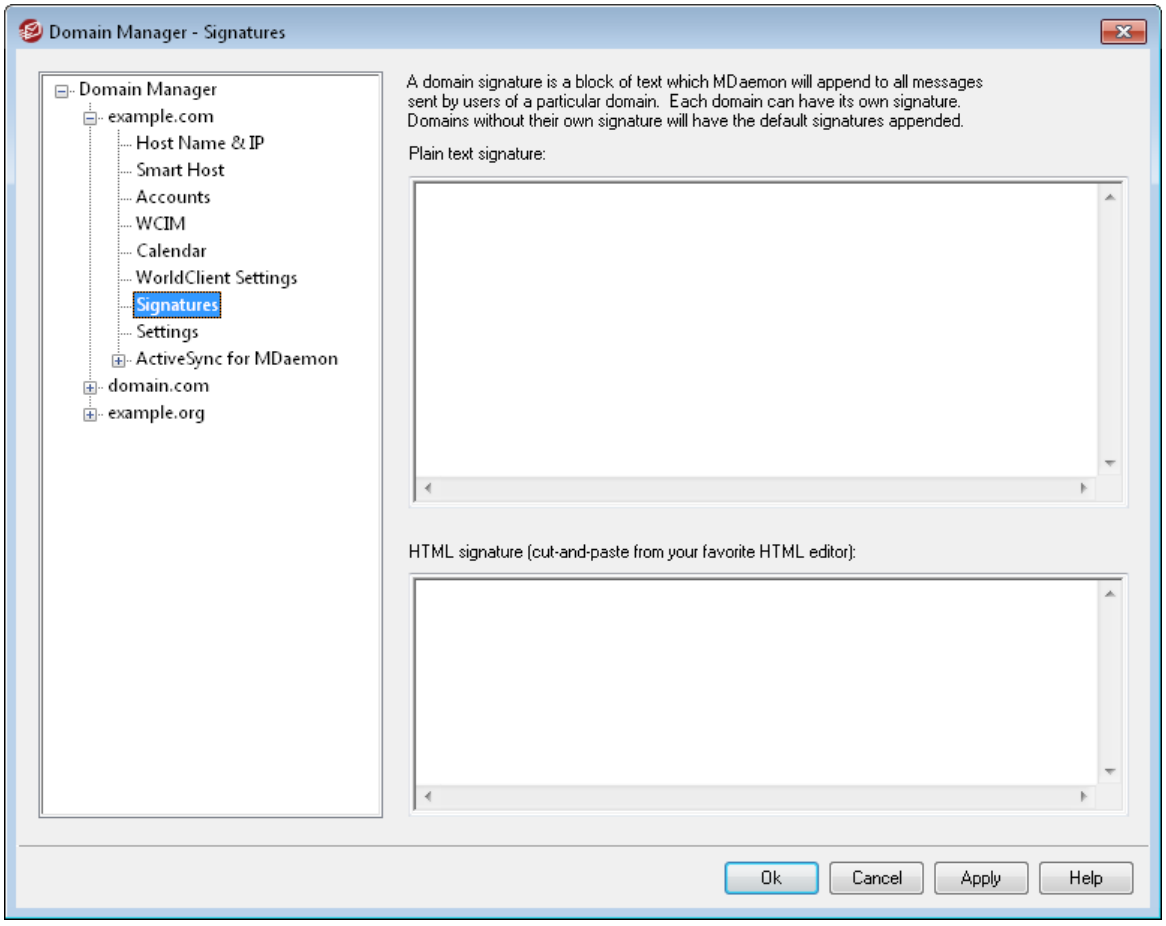
Login failure 'Help' text (can contain HTML code)
You can use this option to specify a sentence of text (either plain text or HTML) to display on the WorldClient sign-in page when a user encounters a problem signing in. The text is displayed below the following default text: "*Incorrect Logon, please try again. If you need assistance please contact your email administrator.*" This text could be used to direct users to a page or contact info for help regarding signing in to WorldClient.

See:

WorldClient (web mail) » Settings 247

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.2.7 Signatures



Use this screen to append a signature to all messages sent by this domain's users. If no signature is specified here then the Default Signature 83 will be appended instead. Signatures are added to the bottom of messages, except for mailing list messages using a footer 206, in which case the footer is added below the signature. You can also use the Account Editor's Signature 568 feature to add individual signatures for each Account. Account signatures are added just before Default or Domain Signatures.

Plain text signature

This area is for inserting a plain text signature. If you wish to designate a corresponding html signature to be used in the text/html part of multipart messages, use the *HTML signature* area below. If a signature is included in both places then MDaemon will use the appropriate one for each part of the multipart message. If no html signature is specified then the plain text signature will be used in both parts.

HTML signature (cut-and-paste from your favorite HTML editor)

This area is for inserting an HTML signature, to be used in the text/html part of multipart messages. If a signature is included both here and in the *Plain text signature* area above, MDaemon will use the appropriate one for each part of the multipart message. If no html signature is specified then the plain text signature will be used in both parts.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

To create your html signature, either type the html code here manually or cut-and-paste it directly from your favorite HTML editor. If you wish to include inline images in your HTML signature, you can do so by using the `$ATTACH_INLINE:path_to_image_file$` macro.

For example:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

There are also several ways you can insert inline images into Default 83 and Domain Signatures from within MDaemon's Remote Administration 251 web interface:

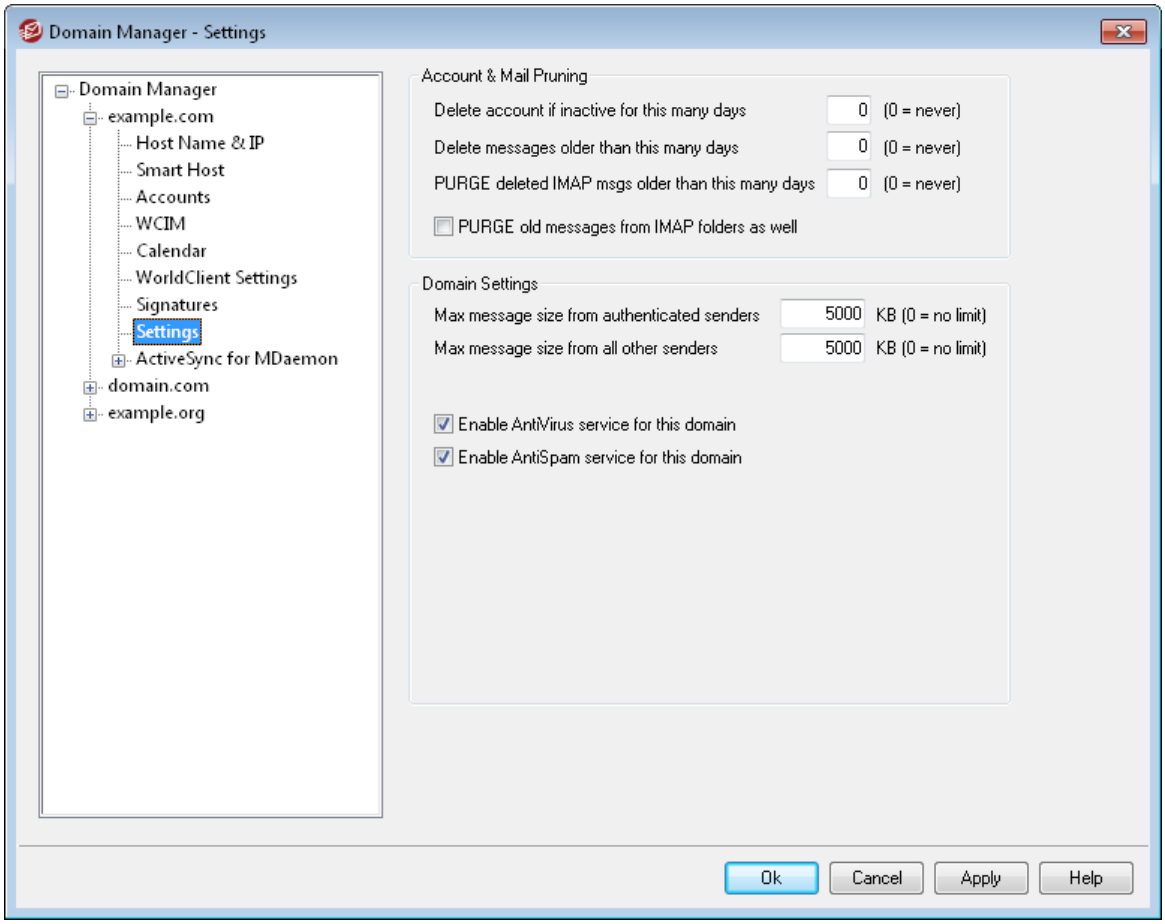
- On the Signature/Footer screen in Remote Administration, click the "Image" toolbar button in the HTML editor and select the upload tab
- On the Signature/Footer screen in Remote Administration, click the "Add image" toolbar button in the HTML editor.
- Drag and drop an image into the Signature/Footer screen's HTML editor with Chrome, FireFox, Safari, or MSIE 10+
- Copy and paste an image from the clipboard into the Signature/Footer screen's HTML editor with Chrome, FireFox, MSIE 11+

See:

Default Signatures 83
Account Editor » Signature 568

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.2.8 Settings



Account & Mail Pruning

These options are used to designate when or if inactive accounts or old messages will be deleted by MDaemon. Each day at midnight MDaemon will remove all messages and accounts that have exceeded the time limits stated. There are similar options on the Account Editor's Quotas 537 screen that can be used to override these settings for individual accounts.

When old messages are pruned, MDaemon will not actually delete them, but will move them to the "...\BADMSGS\[Mailbox]\" folder where they can be manually deleted later by the administrator or a nightly process. **Note:** This only applies to pruned old messages. When an account is pruned, it will be deleted along with its messages instead of moved. See AccountPrune.txt in the "...MDaemon\App\" folder for more information and command line options.

Delete account if inactive for this many days (0 = never)
Specify the number of days that you wish to allow an account belonging to this

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

domain to be inactive before it will be deleted. A value of "0" in this control means that accounts will never be deleted due to inactivity.

Delete messages older than this many days (0 = never)
A value specified in this control is the number of days that any given message may reside in a user's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age.

PURGE deleted IMAP msgs older than this many days (0 = never)
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in your users' folders. Messages flagged for deletion longer than this number of days will be purged from their mailboxes. A value of "0" means that messages flagged for deletion will never be purged due to their age.

PURGE old messages from IMAP folders as well
Click this checkbox if you want the "*Delete messages older than...*" control to apply to messages in IMAP folders as well. When this control is disabled, messages contained in IMAP folders will not be deleted, regardless of their age.

Domain Settings

Max message size from authenticated senders [xx] KB (0=no limit)
Use this option if you wish to set a limit on the size of messages that an authenticated sender can send to the domain. The value is in Kilobytes and set to "0" by default, which means no limit. If you wish to set a message size limit for non-authenticated senders, use the "*...all other senders*" option below.

Max message size from all other senders [xx] KB (0=no limit)
Use this option if you wish to set a limit on the size of messages that a non-authenticated sender can send to the domain. The value is in Kilobytes and set to "0" by default, which means no limit. If you wish to set a message size limit for authenticated senders, use the previous option.

Enable AntiVirus service for this domain
If *SecurityPlus for MDaemon* 362 is installed, click this check box if you want the SecurityPlus settings to be applied to this domain.

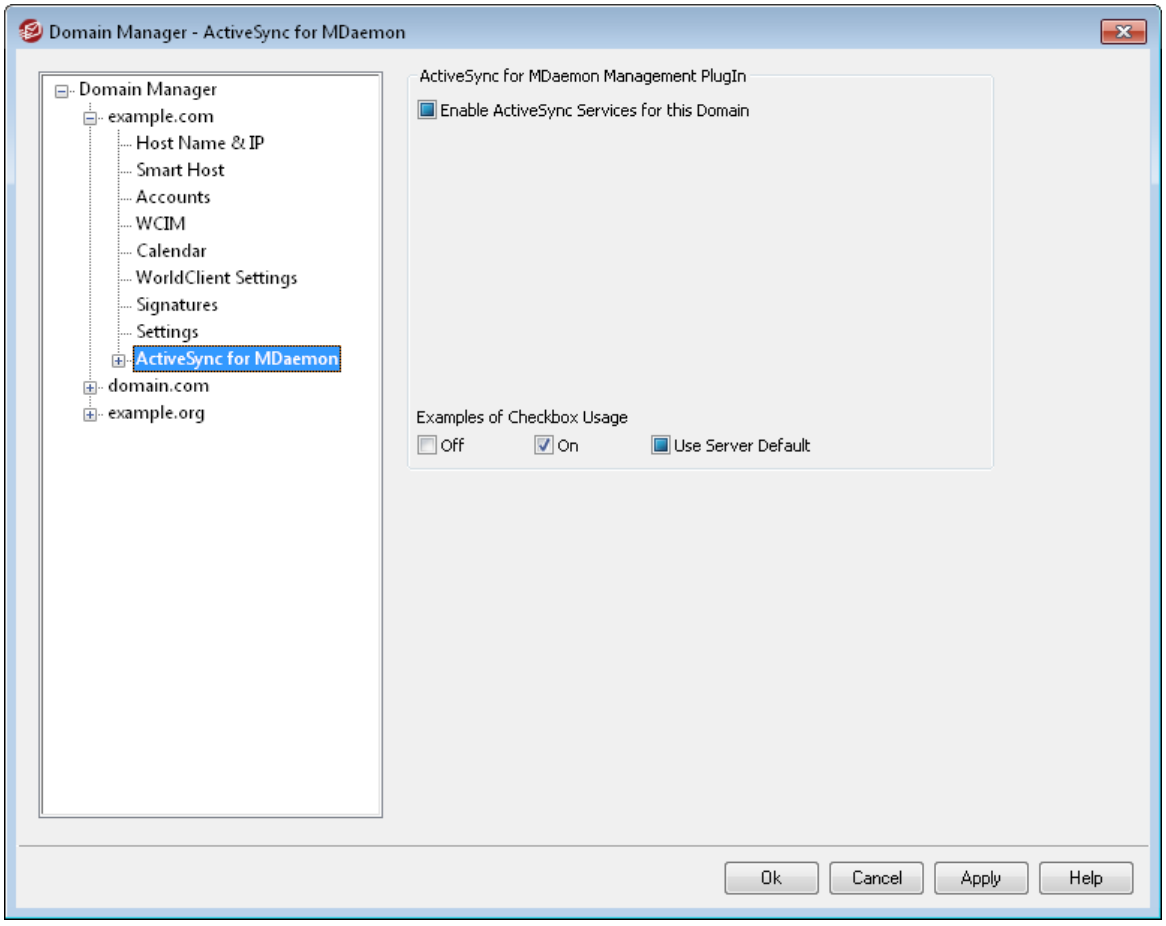
Enable AntiSpam service for this domain
Click this check box is you want MDaemon's current Spam Filter settings to be applied to this domain.

See:

Account Editor » Quotas 537

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.2.9 ActiveSync for MDaemon



Use this section of the Domain Manager to administer a domain's ActiveSync for MDaemon 276 settings. You can manage all domains and domain defaults from the Domains 292 screen under Mobile Device Management.

ActiveSync for MDaemon Management Plugin

Enable ActiveSync Service for this Domain
This option controls whether or not the domain's users will by default be able to use an ActiveSync client to access their email and PIM data. By default the state of this setting is inherited from the Default ActiveSync State 292, but you can override that setting if you choose by toggling the checkbox to either on or off. This setting can also be overridden for any accounts 303 or clients 297 that you do not wish to use the domain's setting.

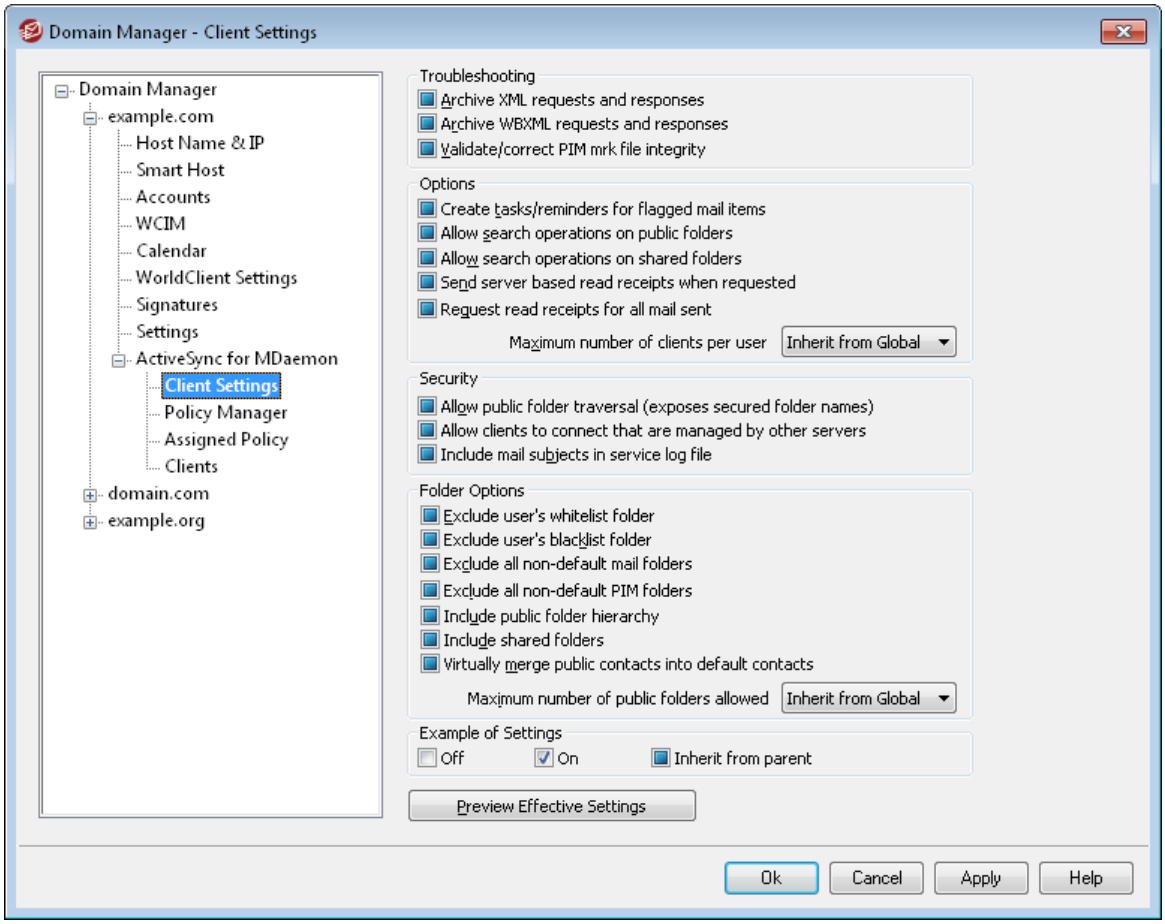
The global option to **Enable ActiveSync for MDaemon Service** 276 must be enabled in order for ActiveSync to be accessible to any of your accounts. The domain-level setting simply controls whether or not any of the domain's accounts will be permitted to use it by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

ActiveSync » Domains 292
ActiveSync » Accounts 303
ActiveSync » Clients 297

3.2.9.1 Client Settings



This screen allows you to manage the default settings for accounts and clients associated with the domain. By default all of the options on this screen are set to "Inherit from parent," which means that each option will take its setting from the corresponding option on the global Client Settings 280 screen. Similarly, this domain's accounts 304 will inherit their settings from this screen, since it is their parent screen. Any changes made to the options on this screen will be reflected on those account screens. Below that, individual clients 156 also have settings screens that inherit their settings from the account-level settings. This configuration makes it possible for you to make changes to all of the domain's accounts and clients simply by making changes to this one screen, while also making it possible for you to override those settings for any account or client as needed.

Troubleshooting

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Archive [XML | WBXML] requests and responses
Use the *Archive XML...* and *Archive WBXML...* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Options

Create Tasks/Reminders for flagged mail items
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email. This is disabled by default.

Allow search operations on Public Folders
Allows the client to search the Public Folders 218 to which it has access. This is allowed by default.

Allow search operations on Shared Folders
Allows the client to search the Shared Folders 547 to which it has access. This is allowed by default.

Send server based read receipts when requested.
Enable this option if you want the server to support read confirmation requests an issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Request read receipts for all mail sent
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Maximum number of clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default.

Security

Allow Public Folder traversal (exposes secured folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 220 for both the subfolder (i.e. child folder) and all parent public folders 218 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Allow clients to connect that are managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Disable this option if you do not wish to allows those clients to connect.

Include mail subjects in service log file
Enable this option if you wish to include each message's Subject header in the ActiveSync log file. This is not recommended, and this option is disabled by default.

Folder Options

Exclude user's [whitelist/blacklist] folder
By default the user's whitelist and blacklist contact folders are not synced with devices. They are generally only used by MDaemon, to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Exclude all non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Exclude all non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include Public Folder hierarchy
Check this box if you want the public folders 218 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Include shared folders
Check this box if you want the shared folders 87 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Virtual merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Maximum number of Public Folders allowed
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

the order in which folders will be processed. By default there is no global limit set.

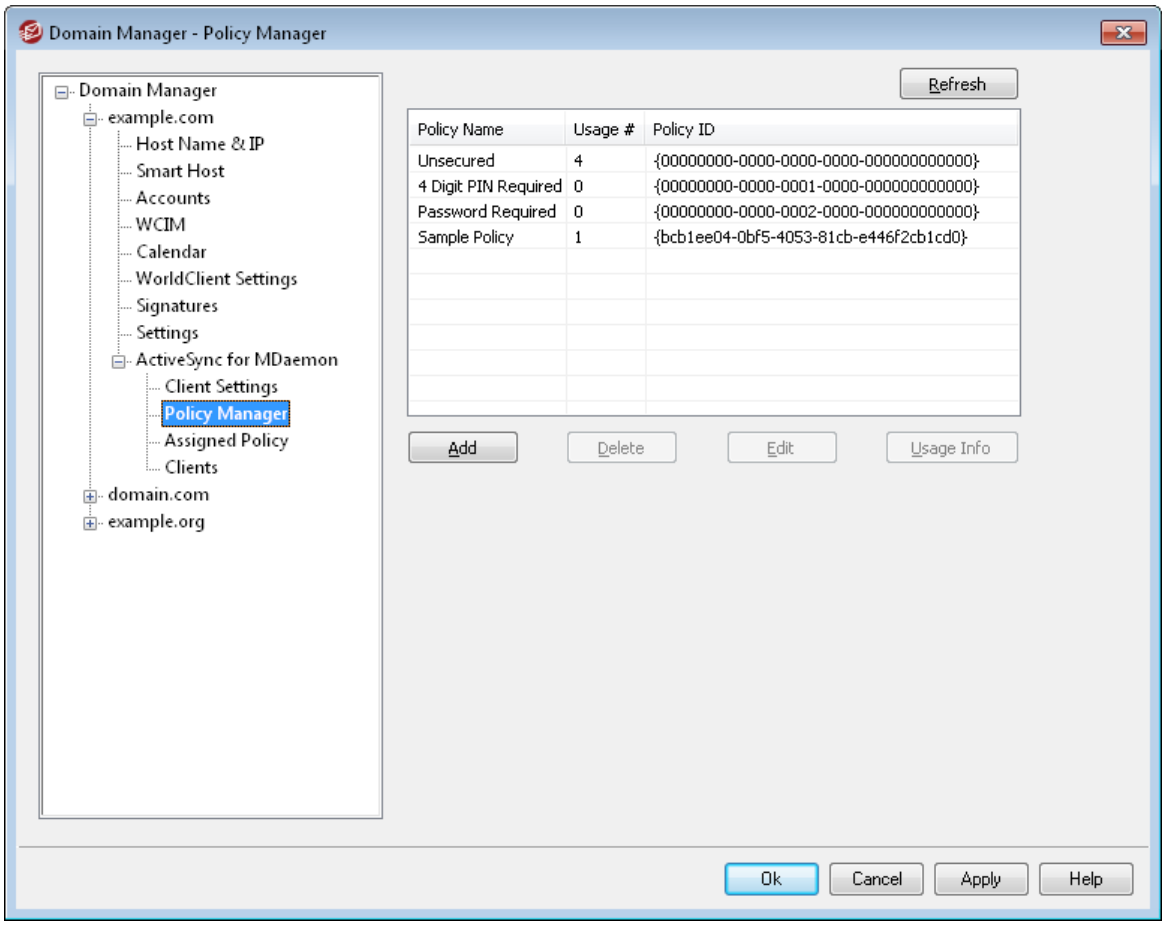
Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 292, accounts 303, and clients 297). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Client Settings 280
ActiveSync » Accounts 303
ActiveSync » Clients 297

3.2.9.2 Policy Manager



Use this screen to manage the ActiveSync Policies that can be assigned to user devices to govern various options. Predefined policies are provided, and you can create, edit and delete your own. Default and overriding policies can can be assigned to the domain and each account 303 and client 297 on their respective Assigned Policy screens.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Not all ActiveSync devices recognize or apply policies consistently. Some may ignore policies or certain policy elements altogether, and others may require a device reboot before changes take effect. Further, when attempting to assign a new policy to a device, it will not be applied to the device until the next time it connects on its own to the ActiveSync server; policies cannot be "pushed" to devices until they connect.

ActiveSync Policies

Add
Click this button to open the ActiveSync Policy Editor, used for creating and editing your policies.

Delete
To delete a policy, select a custom policy from the list and then click **Delete**. Click **Yes** to confirm the action. The predefined policies cannot be deleted.

Edit Policy
To edit a policy, select a custom policy from the list and then click **Edit**. After making your desired changes in the policy editor, click **OK**. The predefined policies cannot be edited.

Usage Info
Select a policy and then click this button to view a list of all domains, accounts, and clients that are set to use this policy.

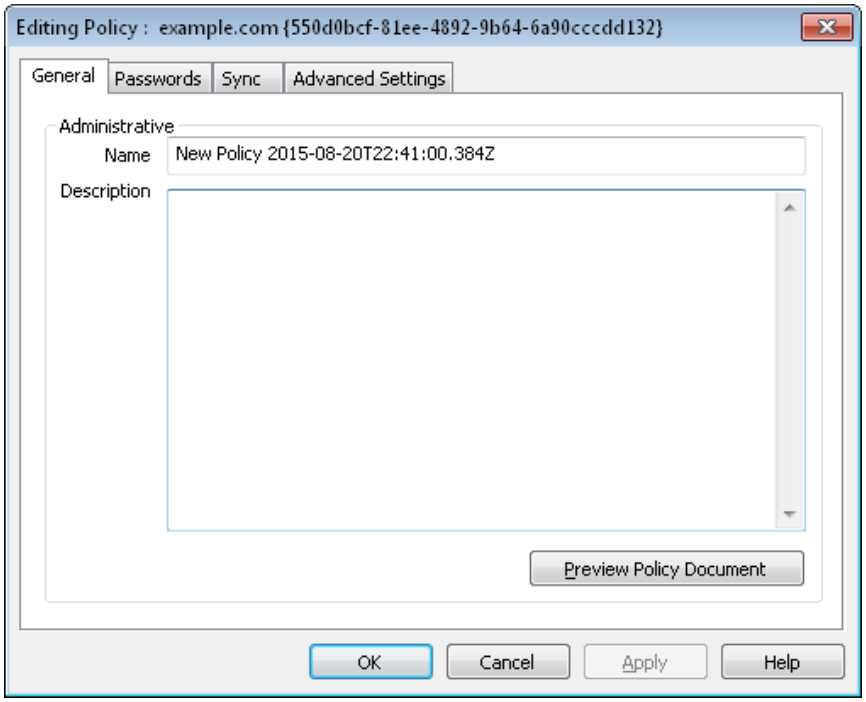
ActiveSync Policy Editor

The ActiveSync Policy Editor has four tabs: General, Passwords, Sync, and Advanced Settings. The Advanced Settings tab is hidden unless you activate *Enable editing of advanced policy options* 276, located on the ActiveSync for MDaemon screen.

General

Use this screen to designate a name and description for your policy. You can also preview the XML policy document.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Administrative

Name
Specify a name for your custom policy here.

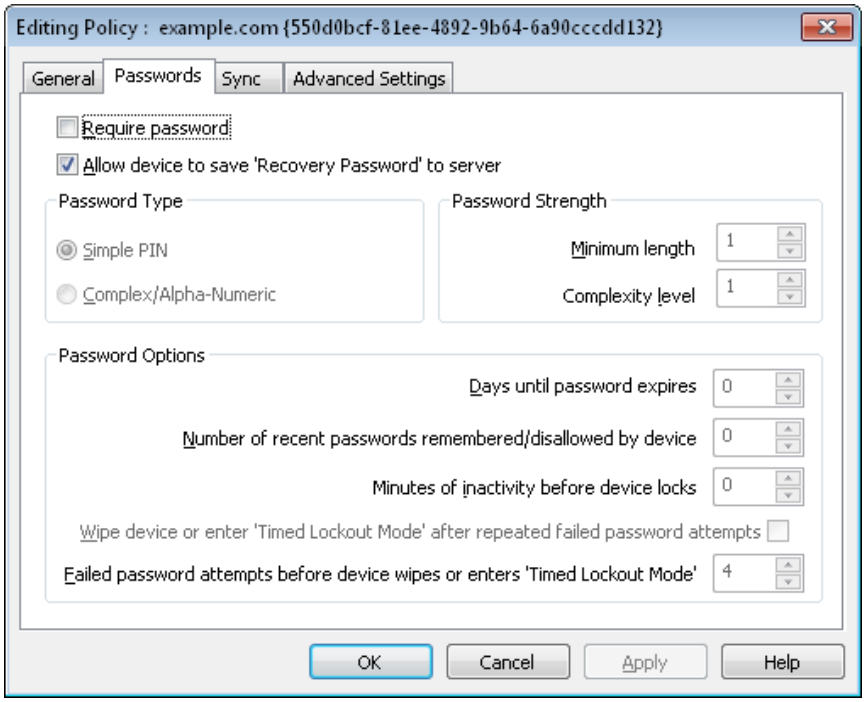
Description
Use this area to describe your custom policy. This description appears on the Apply Policy dialog when selecting a policy to apply to a domain, account, or client.

Preview Policy Document
Click this button to preview the XML policy document for this policy.

Passwords

Password options and requirements for the policy are designated on this tab.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Require password
Check this box if you wish to require a password on the device. It is disabled by default.

Allow device to save 'Recovery Password' to server
Enable this option if you wish to allow clients to use ActiveSync's Recovery Password option, which allows a device to save a temporary recovery password to the server to unlock the device if the password is forgotten. The administrator can find this recover password under the client's Details 297. Most devices do not support this feature.

Password Type

Simple PIN
How this option is implemented is largely dependent on the device, but selecting *Simple PIN* as the password type generally means that no restrictions or complexity requirements are placed on the device password, other than the *Minimum password length* option below. This allows simple passwords such as: "111," "aaa," "1234," "ABCD" and the like.

Complex/Alpha-Numeric
Use this policy option if you wish to require more complex and secure device passwords than the *Simple PIN* option. Use the *Complexity level* option below to define exactly how complex the password must be. This is the default selection when a password is required by the policy.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Password Strength

Minimum length
Use this option to set the minimum number of characters that the device password must contain, from 1-16. This option is set to "1" by default.

Complexity level
Use this option to set the complexity level requirement for *Complex/Alpha-numeric* device passwords. The level is the number of different types of characters that the password must contain: uppercase letters, lowercase letters, numbers, and non-alphanumeric characters (such as punctuation or special characters). You can require from 1-4 character types. For example, if this option were set to "2", then the password must contain at least two of the four character types: uppercase and numbers, uppercase and lowercase, numbers and symbols, and so on. This option is set to "1" by default.

Password Options

Days until password expires (0=never)
This is the number of days allowed before the device's password must be changed. This option is disabled by default (set to "0").

Number of recent passwords remembered/disallowed by device (0=none)
Use this option if you wish to prevent the device from reusing a specified number of old passwords. For example, if this option is set to "2" and you change your device password, you will not be able to change it to either of the last two passwords that were used. The option is disabled by default (set to "0").

Minutes of inactivity before device locks (0=never)
This is the number of minutes that a device can go without any user input before it will lock itself. This password option is disabled by default (set to "0").

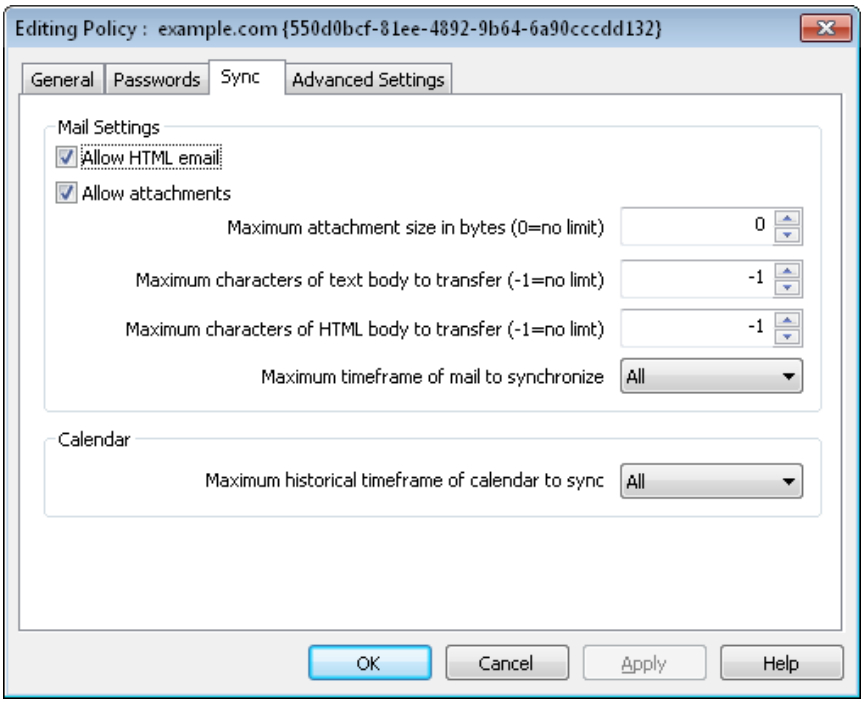
Wipe device or enter 'Timed Lockout Mode' after repeated failed password attempts
When this option is enabled and the user fails the designated number of password attempts, the device will either lock itself for a certain amount of time or perform a wipe of all data, depending on the device. This option is disabled by default.

Failed password attempts before device wipes or enters 'Timed Lockout Mode'
When the "*Wipe device..*" option above is enabled and a user fails this many password attempts, the device will be wiped or the 'Timed Lockout Mode' will be triggered, depending on the device.

Sync

This screen contains various settings governing HTML email, allowing attachments, limiting the number of characters to transfer, and the maximum mail and calendar timeframes to sync.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Mail Settings

Allow HTML email
By default HTML-formatted email can be synced/sent to ActiveSync clients. Uncheck this box if you wish to send only plain text.

Allow attachments
Allows the device to download file attachments. This option is enabled by default.

Max attachment size in bytes (0=no limit)
This is the maximum size of attachment that can be automatically downloaded to the device. There is no size limit set for this option by default (set to "0").

Maximum characters of text body to transfer (-1=no limit)
This is the maximum number of characters in the body of plain text-formatted emails that will be sent to the client. If the message body contains more characters than are allowed, the body will be truncated to the specified limit. By default there is no limit set (option set to "-1"). If you set the option to "0" then only the message header is sent.

Maximum characters of HTML body to transfer (-1=no limit
This is the maximum number of characters in the body of HTML-formatted emails that will be sent to the client. If the message body contains more characters than are allowed, the body will be truncated to the specified limit. By default there is no limit set (option set to "-1"). If you set the option to "0" then only the message header is sent.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

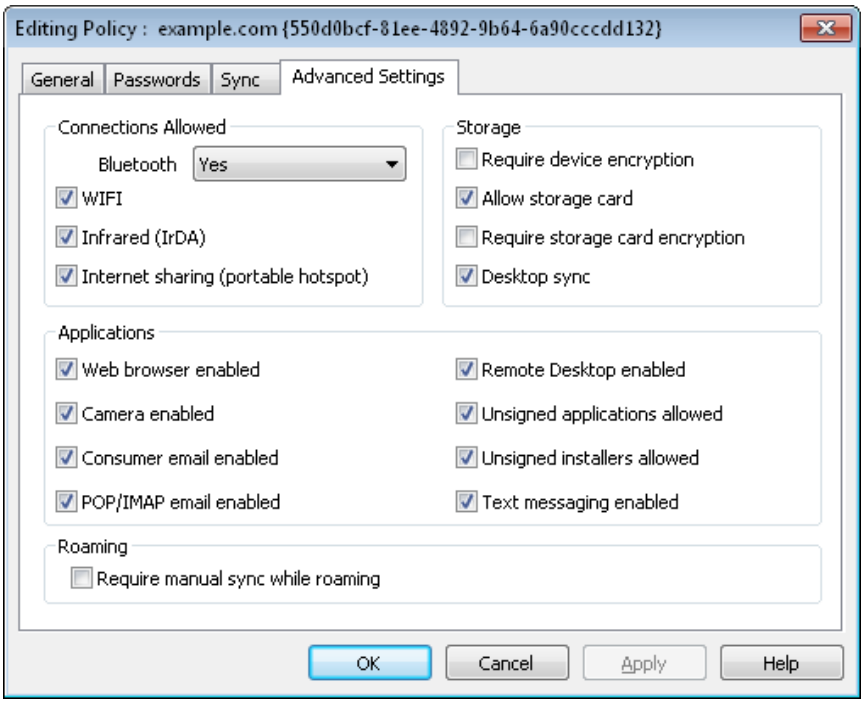
Maximum timeframe of mail to synchronize
This is the amount of past email, by date range from today, that can be synchronized by the device. By default this is set to "All," meaning that all email can be synchronized no matter how old it is.

Calendar

Maximum historical timeframe of calendar to sync
This is how far back from today that past calendar entries can be synchronized by the device. By default this is set to "All," meaning that all past entries can be synchronized no matter how old they are.

Advanced Settings

The Advanced Settings tab contains options governing the types of connections allowed, whether certain applications can be enabled, storage and encryption, and roaming.



This tab is hidden unless you activate *Enable editing of advanced policy options* 276, located on the ActiveSync for MDaemon screen.

Connections Allowed

Bluetooth
Use this option to designate whether or not Bluetooth connections are allowed on the device. You can choose **Yes** to allow Bluetooth connections, **No** to prevent them, or **Handsfree** to restrict Bluetooth to Handsfree only. This option is set to **Yes** by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

WIFI
Allows WIFI connections. Enabled by default.

Infrared (IrDA)
Allows Infrared (IrDA) connections. Enabled by default.

Internet sharing (portable hotspot)
This option allows the device to use Internet sharing (portable hotspot). It is enabled by default.

Storage

Require device encryption
Click this option if you wish to require encryption on the device. Not all devices will enforce encryption. This is disabled by default.

Allow storage card
Allows a storage card to be used in the device. This is enabled by default.

Require storage card encryption
Use this option if you wish to require encryption on a storage card. This is disabled by default.

Desktop sync
Allows Desktop ActiveSync on the device. Enabled by default.

Applications

Web browser enabled
Allows the use of a browser on the device. This option is not supported on some devices, and it may not apply to 3rd party browsers. It is enabled by default.

Camera enabled
Allows the use of a camera on the device. This option is enabled by default.

Consumer email enabled
Device allows the user to configure a personal email account. When disabled, the types of email accounts or services that are prohibited is entirely dependent on the particular ActiveSync client. This option is enabled by default.

POP/IMAP email enabled
Allows access to POP or IMAP email. Enabled by default.

Remote Desktop enabled
Allows the client to use Remote Desktop. Enabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Unsigned applications allowed
This option allows unsigned applications to be used on the device. This is enabled by default.

Unsigned installers allowed
This option allows unsigned installers to be run on the device. This is enabled by default.

Text messaging enabled
This option allows text messaging on the device. Text messaging is enabled by default.

Roaming

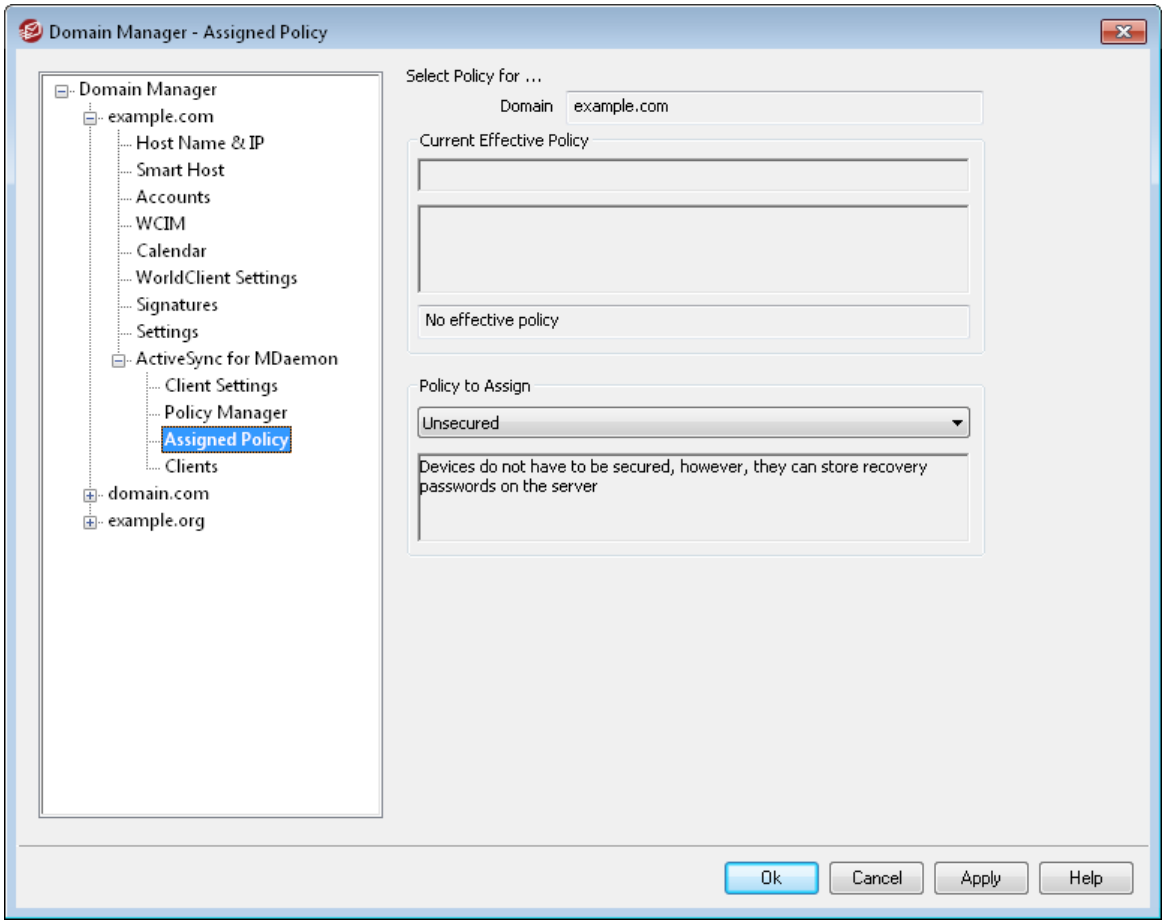
Require manual sync while roaming
Use this policy option if you wish to require the device to synchronize manually while roaming. Allowing automatic synchronization while roaming could increase data costs for the device, depending on its carrier and data plan. This option is disabled by default.

See:

Domain Manager » Assigned Policy 155
ActiveSync » Accounts 303
ActiveSync » Clients 297

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.2.9.3 Assigned Policy



Use this screen to assign the default ActiveSync policy 146 for the domain. When an ActiveSync client connects using one of this domain's accounts, this is the policy that will be assigned to the client, unless an alternate policy has been set specifically for that account.

Assigning a Default ActiveSync Policy

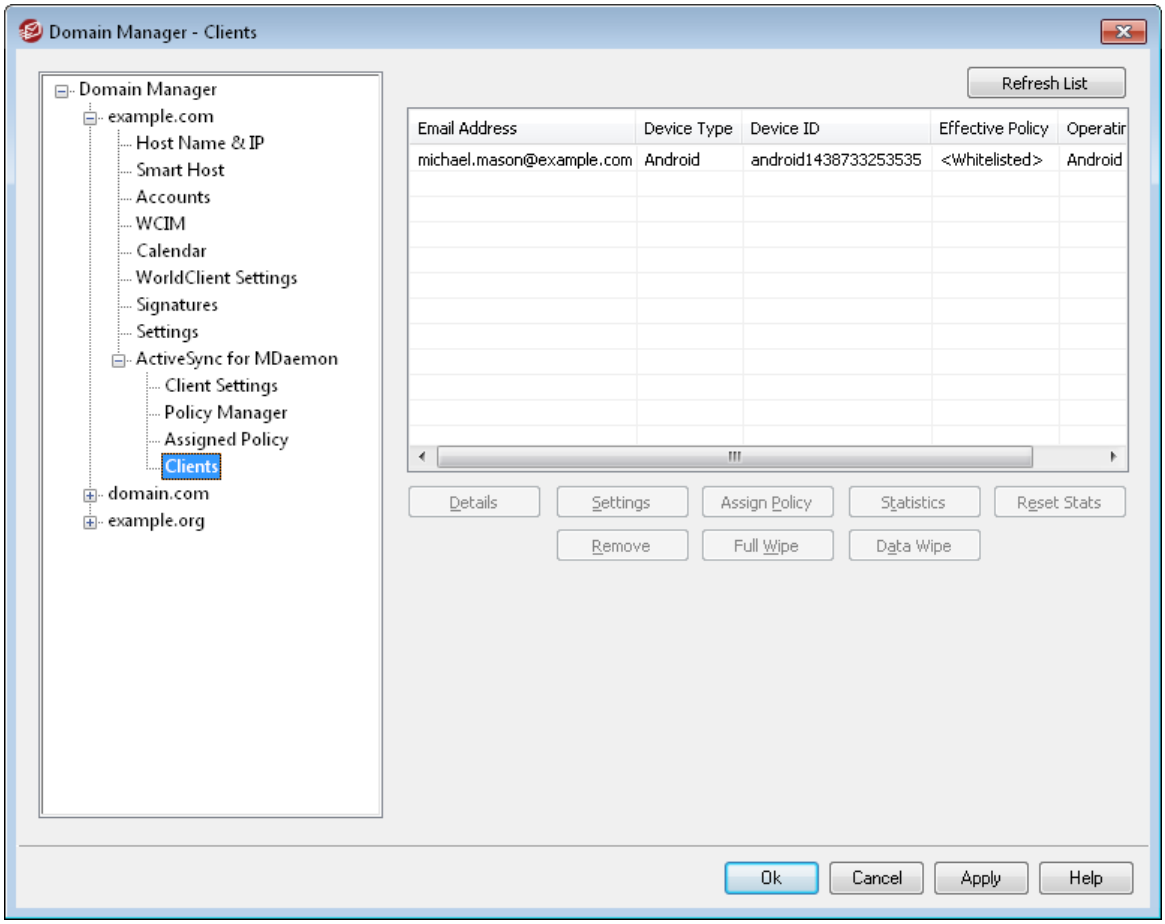
To assign a default ActiveSync policy for the domain, click the **Policy to Assign** drop-down list, select the desired policy, and click **Ok**.

See:

Domain Manager » Policy Manager 146
ActiveSync » Accounts 303
ActiveSync » Clients 297

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

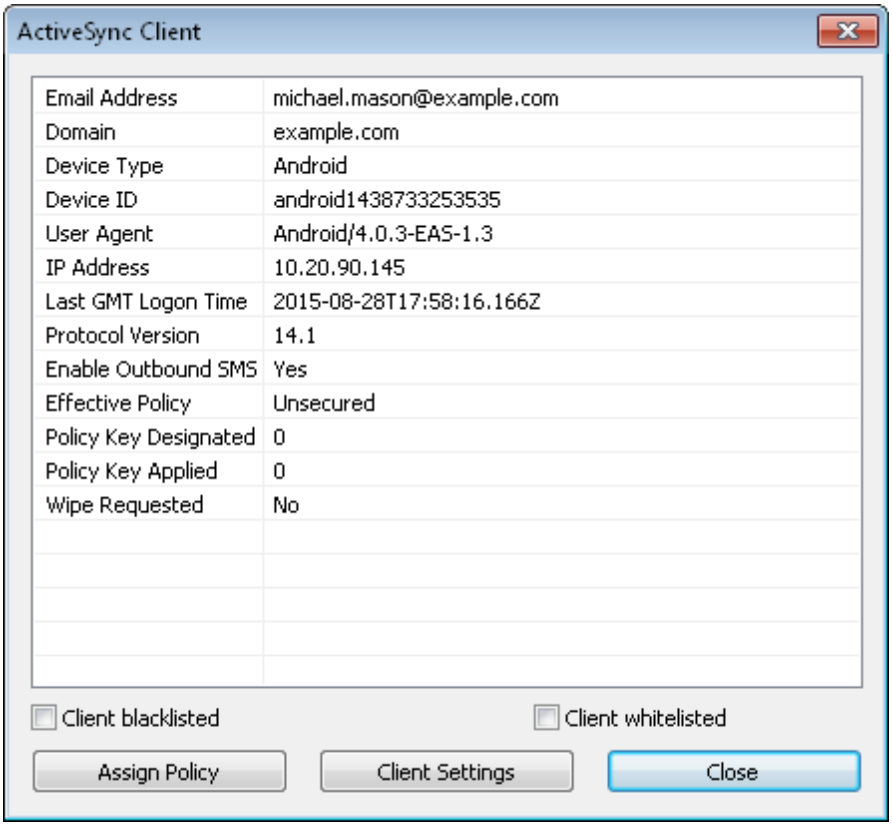
3.2.9.4 Clients



This screen contains an entry for each ActiveSync device associated with the domain. Double-click any entry to see more details about the device.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Details



Select an entry and click **Details** (or double-click the entry) to open the Client Details dialog. On this screen you can view information about the device, assign a policy, access its client settings, or add the device to the blacklist or whitelist 308.

Device Settings

Select a device and click **Settings** to manage the Client Settings for the device. By default these settings are inherited from the account's 303 Client Settings screen. See Managing a Device's Client Settings below.

Assigning an ActiveSync Policy

To assign a Policy 284 to the device:

1. Select a device from the list.
2. Click **Assign Policy**. This opens the Apply Policy dialog.
3. Click the Assigned Policy drop-down list and choose the desired policy.
4. Click **OK**.

Statistics

Click **Statistics** to open the Device Statistics dialog, containing various usage stats for the device.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Reset Stats

If you wish to reset the device's stats, click **Reset Stats**, and **Ok** to confirm the action.

Removing an ActiveSync Device

To remove an ActiveSync device, select the device and click *Remove*. This will remove the device from the list and delete all synchronization information related to it in MDaemon. Therefore if in the future the account uses ActiveSync to synchronize the same device, MDaemon will treat the device as if it had never before been used on the server; all device data will have to be re-synchronized with MDaemon.

Full Wiping an ActiveSync Device

To do a Full Wipe on an ActiveSync device, select the device from the list and click *Full Wipe*. The next time the device connects, MDaemon will tell it to erase all data, or restore itself to its factory default state. Depending on the device, this may remove everything on it, including downloaded apps. Further, as long as the device's ActiveSync entry exists in MDaemon, it will be wiped again if it ever connects again to MDaemon in the future. If you no longer wish to wipe the device when it connects (for example, if a lost device is recovered and you wish to use it again with the account) then you must first use the *Remove* option above to remove the device from MDaemon.

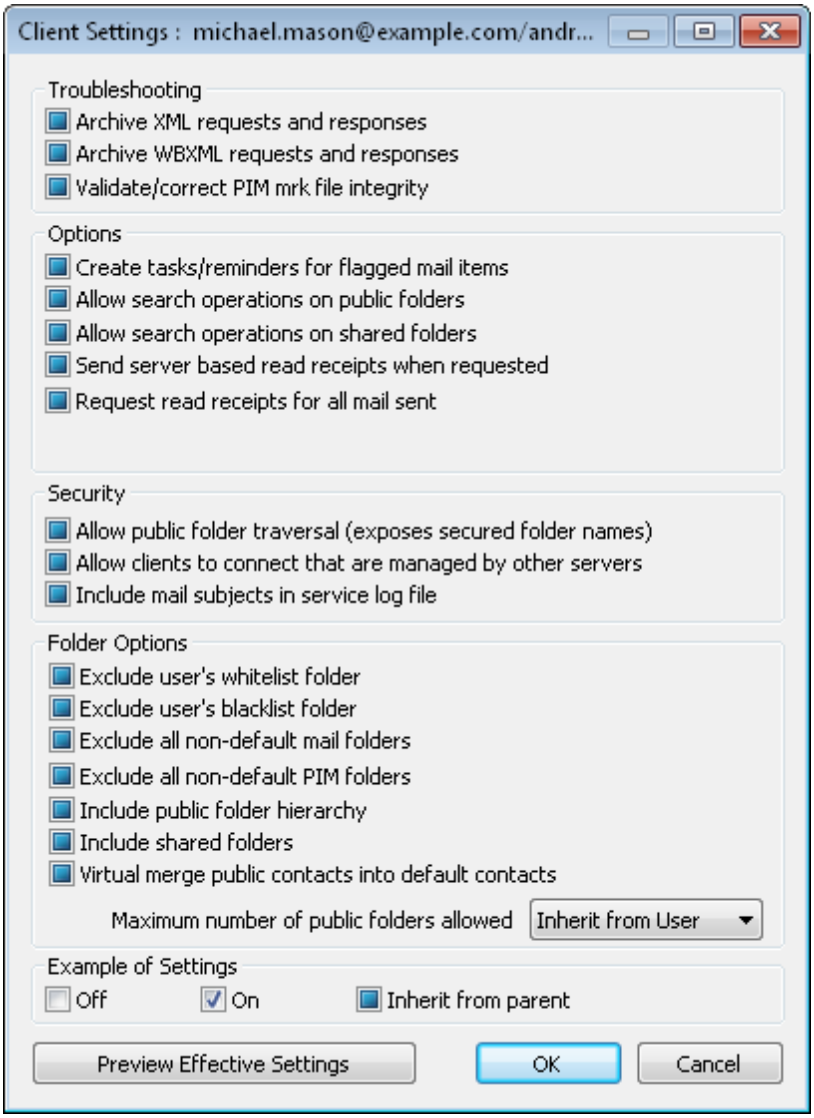
Data/Soft Wiping an ActiveSync Device

The *Data Wipe* (or *Soft Wipe*) option is similar to the *Full Wipe* option explained above, but instead of wiping all data, it will wipe only the account's data, such as its emails, calendar entries, contacts, and the like. The rest, such as apps, photos or music is left alone.

Managing a Device's Client Settings

The device-level Client Settings screen allows you to manage settings for a specific device.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.


Client Settings : michael.mason@example.com/andr...
Troubleshooting
Archive XML requests and responses
Archive WBXML requests and responses
Validate/correct PIM mrk file integrity
Options
Create tasks/reminders for flagged mail items
Allow search operations on public folders
Allow search operations on shared folders
Send server based read receipts when requested
Request read receipts for all mail sent
Security
Allow public folder traversal (exposes secured folder names)
Allow clients to connect that are managed by other servers
Include mail subjects in service log file
Folder Options
Exclude user's whitelist folder
Exclude user's blacklist folder
Exclude all non-default mail folders
Exclude all non-default PIM folders
Include public folder hierarchy
Include shared folders
Virtual merge public contacts into default contacts
Maximum number of public folders allowed
Inherit from User
Example of Settings
Off
On
Inherit from parent
Preview Effective Settings
OK
Cancel

By default all of the options on this screen are set to "Inherit from user," which means that each option will take its setting from the corresponding option on the account's Client Settings 303 screen. Any changes made to the settings on that screen will be reflected on this screen. Conversely, any changes you make to this screen will override the account-level setting for this device.

Troubleshooting

Archive [XML | WBXML] requests and responses
Use the *Archive XML...* and *Archive WBXML...* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

UIDs or empty required fields. The global option is disabled by default.

Options

Create Tasks/Reminders for flagged mail items
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email. This is disabled by default.

Allow search operations on Public Folders
Allows the client to search the Public Folders 218 to which it has access. This is allowed by default.

Allow search operations on Shared Folders
Allows the client to search the Shared Folders 547 to which it has access. This is allowed by default.

Send server based read receipts when requested.
Enable this option if you want the server to support read confirmation requests an issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Request read receipts for all mail sent
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Maximum number of clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default.

Security

Allow Public Folder traversal (exposes secured folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 220 for both the subfolder (i.e. child folder) and all parent public folders 218 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Allow clients to connect that are managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Disable this option if you do not wish to allows those clients to connect.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Include mail subjects in service log file
Enable this option if you wish to include each message's Subject header in the ActiveSync log file. This is not recommended, and this option is disabled by default.

Folder Options

Exclude user's [whitelist/blacklist] folder
By default the user's whitelist and blacklist contact folders are not synced with devices. They are generally only used by MDaemon, to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Exclude all non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Exclude all non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include Public Folder hierarchy
Check this box if you want the public folders 218 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Include shared folders
Check this box if you want the shared folders 87 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Virtual merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Maximum number of Public Folders allowed
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 292, accounts 303, and clients 297). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

currently being applied to the displayed screen.

See:

ActiveSync » Accounts 303
ActiveSync » Security 308

3.3 Gateway Manager

The Gateway Manager is an MDaemon PRO feature and is reached from the Setup » Gateway Manager... menu selection. This feature provides a limited yet useful secondary level of support for hosting multiple domains or acting as a backup mail server for someone.

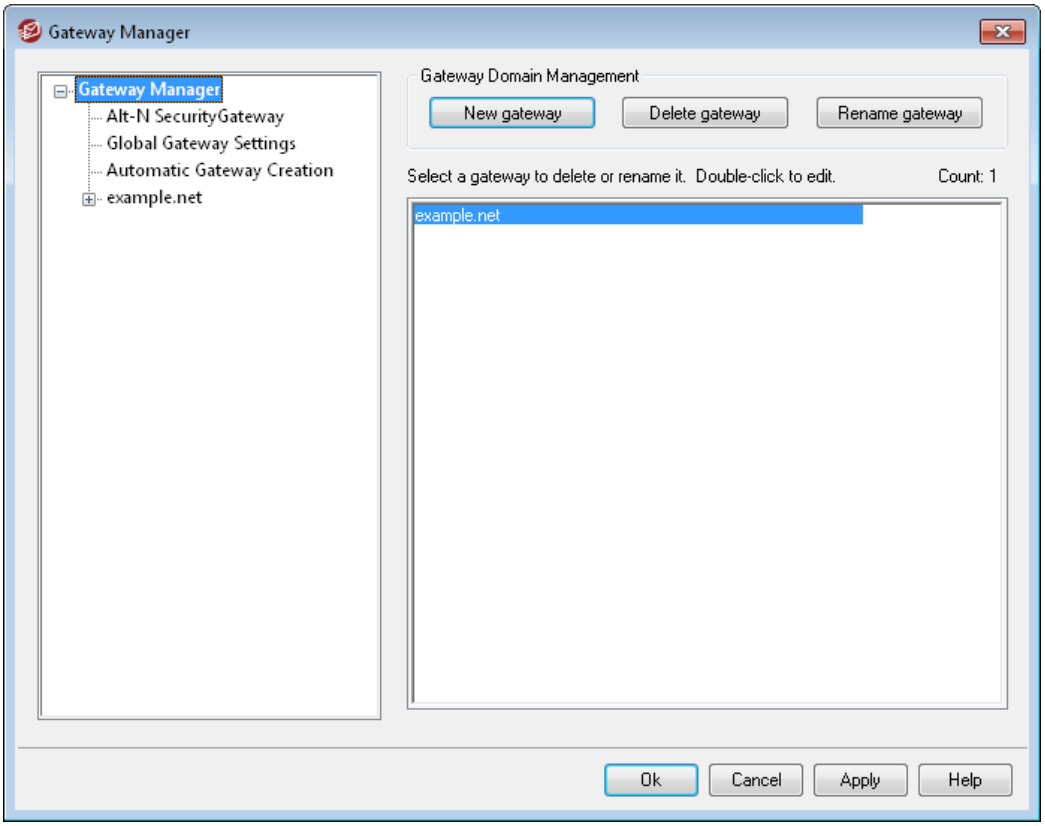
For example:

> Suppose you wish to act as a backup server or mail-drop for a third party, receiving its incoming email and storing it in a folder on your server, but you do not wish to host its domain fully, maintaining its individual user accounts. Let's use "example.com" as its name.
>
> The first thing you will do is create the gateway by clicking **New gateway** on the Gateway Manager and then entering "example.com" as its name. Now all mail that MDaemon receives for that domain will be separated from the main mail stream and placed in the folder designated on the gateway's Domain 168 screen, regardless of the specific individuals to which each message is addressed.
>
> Next, you will designate the collection or delivery methods that you wish to allow or use to get the domain's email to its actual email server, where its user accounts are hosted. There are two ways to do this: use the *Deliver stored messages each time MDaemon processes remote mail* option on the Domain screen 168, or use the Dequeuing 175 options. Optionally, you can also create an MDaemon account and change its Mail Folder 524 to the same storage folder 168 that your gateway uses. This will allow a mail client to connect to MDaemon to collect example.com's email.
>
> Finally, you will likely have to edit the DNS settings for example.com so that your MDaemon server is a designated MX host for that domain.

There are many other features and options available, but the above example is the basic form that a typical gateway will take. If, however, you require an atypical configuration then you may have to do some things differently, such as when you wish to use a domain name that doesn't actually exist on the Internet, like "company.mail." Receiving messages for an otherwise invalid domain name such as that is possible, but the domain name must be "hidden" inside a default domain 121 address. Using that method, addresses can be constructed that will pass through the default domain and on to the gateway. For example, if your default domain is example.com and you have a gateway for company.mail, then someone could send a message to "bob@company.mail" by using the address, "bob{company.mail}@example.com." Since "example.com" is the registered domain hosted by MDaemon, this message would be delivered properly, but when MDaemon received the message in that format it would convert the address to "bob@company.mail" and deliver the message to the folder

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

specified for that gateway. Of course the simplest method is still to register a valid domain name for the gateway and then point its DNS or MX record to `example.com`.



Gateway List

The navigation pane on the left side of this dialog contains the list of your gateways, with links to each screen used for configuring the various gateway-specific settings. It also provides access to the Global Gateway Settings 165 and Automatic Gateway Creation 166 screens. The list on the right is used for deleting and renaming domains. You can double-click a gateway in this list to switch to the gateway editor for configuring its settings.

Gateway Domain Management

New gateway

To create a new gateway: click **New gateway**, enter the gateway name (e.g. example.mail) in the Create/Rename Gateway Domain dialog, and click **OK**.

Typically the value entered here will be the registered Internet domain name that a DNS server resolves to the IP address of the local machine running the server, or a qualified alias of that name. Alternatively, you may choose to use an internal-only or otherwise non-valid, non-public domain name (such as "`company.mail`") for your gateway name. This, however, would require you to use the nested domain name method outlined in the example above, or require you to utilize some other content filtering scheme to get the messages where they belong.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Delete gateway
To delete a gateway: select it from the list and click **Delete gateway**, and click **Yes** to confirm your decision.

Rename gateway
To change a gateway's name: select it from the list, click **Rename gateway**, type the new name in the Create/Rename Gateway Domain dialog, and click **OK**.

Gateway Editor

The Gateway Editor is used for editing each gateway's settings. It includes the following screens:

Domain 168
Use this screen to enable/disable the gateway, designate the folder used for storing the domain's messages, and configure other delivery and attachment-handling options.

Verification 170
If the remote domain's server is configured to keep an LDAP or Active Directory server up to date with all of its mailboxes, aliases, and mailing lists, or if it runs a Minger server to provide remote address verification, you can use this dialog to specify that server and thus verify the validity of recipient addresses of incoming messages. When a recipient address is found to be invalid the message will be rejected. With this method you can avoid having to assume that all recipients of a domain's messages are valid.

Forwarding 174
With this screen you can declare a host or address to which the domain's mail will be forwarded as soon as it arrives. There are also options for stating whether a copy of these messages should be kept locally and for designating the port on which the forwarded messages should be sent.

Dequeuing 175
Using the options on this screen, you can configure MDaemon to respond to ETRN and ATRN requests made on behalf of the domain in order to dequeue its messages. You can also configure several other dequeuing related options.

Quotas 177
This dialog is used for assigning a limit to the amount of disk space that the domain may use and the maximum number of messages that may be stored.

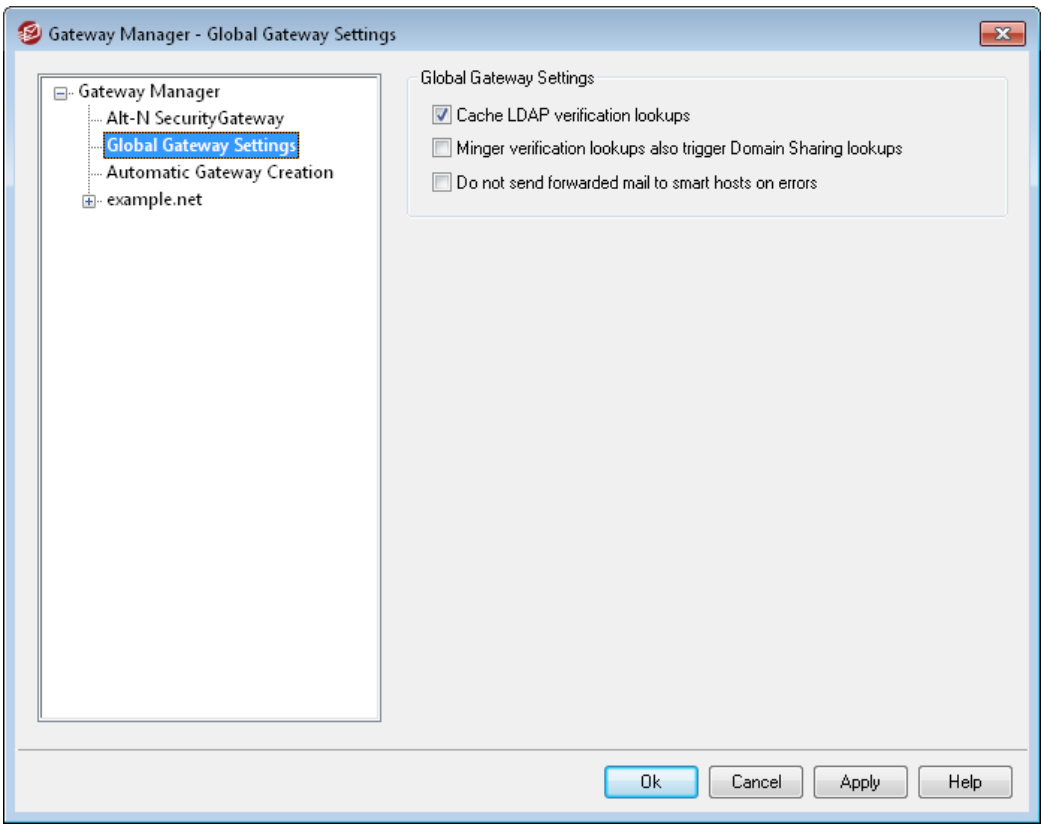
Settings 179
This screen contains a number of other options that will apply to the selected domain gateway. For example, you can enable/disable AntiVirus and AntiSpam scanning for the gateway, designate whether or not authentication is required when dequeuing mail, designate an authentication password, and several other options.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Global Gateway Settings 165
Automatic Gateway Creation 166
Domain Manager 121

3.3.1 Global Gateway Settings



Global Gateway Settings

The following options are global options. They aren't limited to any particular gateway.

Cache LDAP verification lookups
Click this checkbox if you wish to cache the results of LDAP verification 170 queries for your domain gateways.

Minger verification lookups also trigger Domain Sharing lookups
When this option is enabled and Minger 640 is used by any of your gateways for address verification, in addition to querying the Minger host designated on the Verification screen 170, MDaemon will also query your Domain Sharing 75 hosts. This option applies to all gateways set to use Minger for address verification.

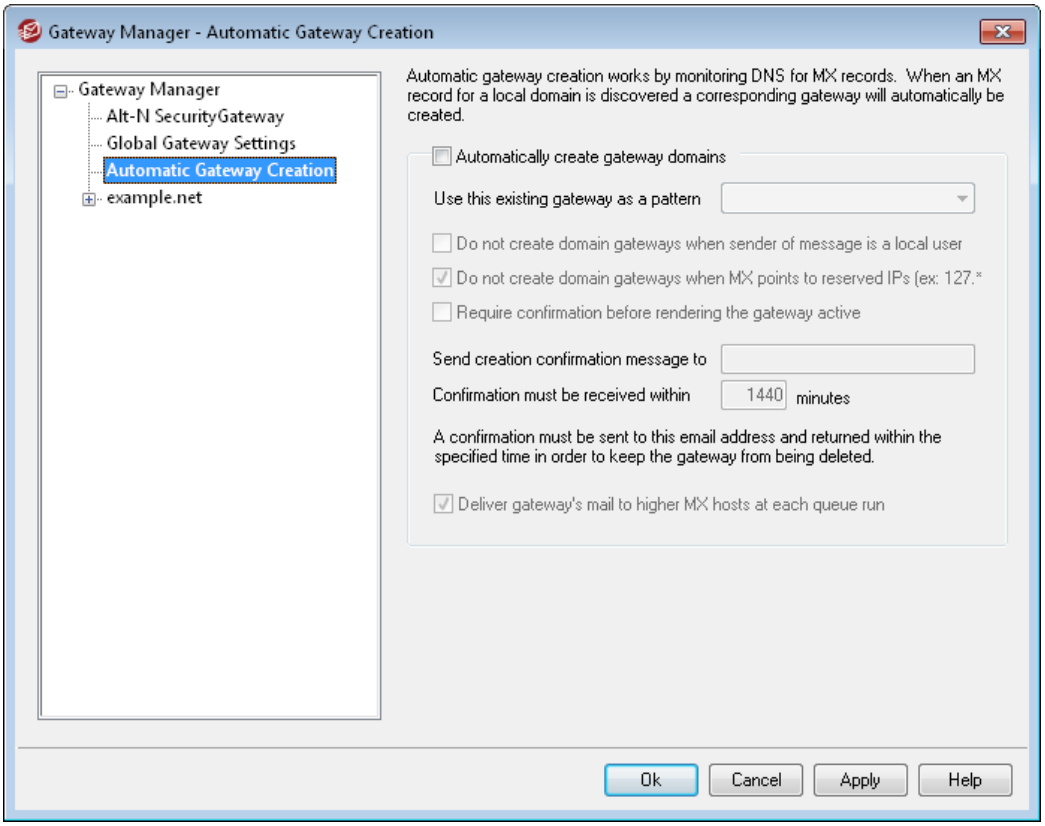
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Do not send forwarded mail to smart host on errors
Click this option to prevent the sending of forwarded emails to the host specified above when delivery errors occur. This option is disabled by default.

See:

Gateway Manager 162
Gateway Editor » Verification 170
Minger 640
Domain Sharing 75

3.3.2 Automatic Gateway Creation


Gateway Manager - Automatic Gateway Creation
Gateway Manager
Alt-N SecurityGateway
Global Gateway Settings
Automatic Gateway Creation
example.net
Automatic gateway creation works by monitoring DNS for MX records. When an MX record for a local domain is discovered a corresponding gateway will automatically be created.
Automatically create gateway domains
Use this existing gateway as a pattern
Do not create domain gateways when sender of message is a local user
Do not create domain gateways when MX points to reserved IPs (ex: 127.*
Require confirmation before rendering the gateway active
Send creation confirmation message to
Confirmation must be received within
1440
minutes
A confirmation must be sent to this email address and returned within the specified time in order to keep the gateway from being deleted.
Deliver gateway's mail to higher MX hosts at each queue run
Ok
Cancel
Apply
Help

Automatic Gateway Creation (MDaemon PRO only)

This feature is used to automatically create a Domain Gateway 162 for a previously unknown domain when another source attempts to deliver that domain's messages to MDaemon, and a DNS query lists MDaemon's location as a valid MX record.

For example:

With automatic gateway creation enabled, if MDaemon's Default Domain IP address is `192.0.2.0` and a message is delivered via SMTP for an unknown domain `example.com`, MDaemon will perform MX and A-record queries on `example.com` to see if `192.0.2.0` is a known mail relay host for it. If the results of the DNS queries state that MDaemon's

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

IP address is a valid MX host for `example.com` then MDaemon will automatically create a new Domain Gateway for it and accept its email. Messages for `example.com` will then be stored in a special folder and, if you so choose, spooled to higher level MX hosts at each remote mail processing interval. This feature effectively enables you to become a backup server for another domain by simply configuring the DNS system to use your IP as an alternate MX host.

To help secure this feature, MDaemon can be configured to send a confirmation request to an email address of your choice. While MDaemon is waiting for the confirmation response, messages for the domain will be accepted and stored but not delivered. Confirmation requests must be replied to within an amount of time that you designate or the automatically created gateway will be removed and all stored messages deleted. If confirmation is received before the time has expired then the stored messages will be delivered normally.

It might be possible for a malicious person or "spammer" to attempt to exploit this feature by configuring their DNS server to list your MDaemon's IP address as one of their MX hosts. Automatic Gateway Creation must therefore be used with caution. To aid in preventing possible exploitation we recommend utilizing the *Send creation confirmation message to...* feature whenever possible.

Automatically create gateway domains
Click this checkbox if you want MDaemon to automatically create Domain Gateways based upon the results of DNS queries.

Use this existing gateway as a pattern
Choose a Domain Gateway from this drop-down list and MDaemon will use its settings as a template for all future automatically created gateways.

Don't create domain gateways when sender of message is a local user
Enable this control if you do not want messages originating from local users to trigger automatic gateway creation.

Don't create domain gateways when MX points to reserved IPs
Click this check box if you wish to prevent an automatic gateway creation when the MX record points to a reserved IP address such as 127.*, 192.*, or the like.

Require confirmation before rendering the gateway active
When this control is enabled, MDaemon will send a confirmation message to the email address of your choice in order to determine whether the automatically created gateway is valid. MDaemon will continue to accept messages for the domain in question but will not deliver them until confirmation is received.

Send creation confirmation message to
Use this text box to designate the email address to which confirmation messages will be sent.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Confirmation must be received within XX minutes
This control is for designating the number of minutes that MDaemon will wait for a response to any given confirmation message. If this time limit expires then the Domain Gateway in question will be deleted.

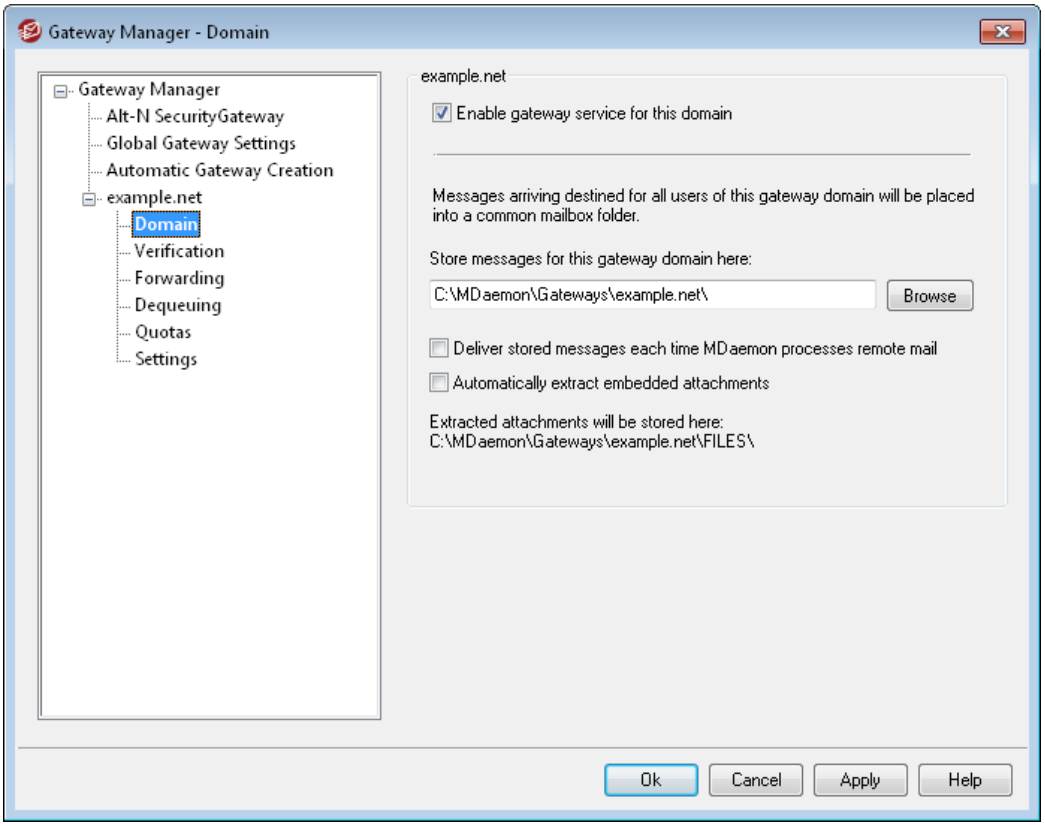
Deliver gateway's mail to higher MX hosts at each queue run
If you want MDaemon to attempt to deliver this gateway's messages to higher level MX hosts each time that the remote queue is processed then enable this control.

See:

Gateway Manager 162

3.3.3 Gateway Editor

3.3.3.1 Domain



Gateway Domain

Enable gateway service for this domain
Check this box to enable the domain gateway.

Store messages for this gateway domain here:
Enter the directory where you wish to store incoming mail for the domain. All of its

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

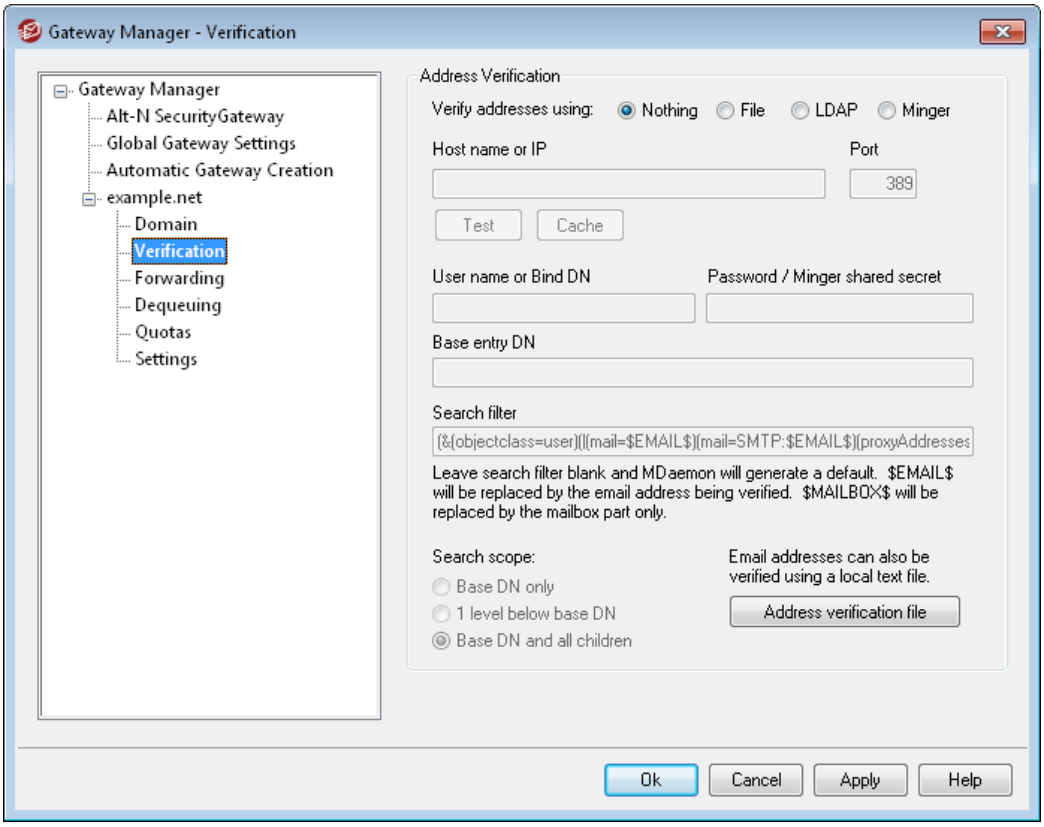
messages will be stored in the same folder regardless of the individual recipients to which each message is addressed.

Deliver stored messages each time MDaemon processes remote mail
Ordinarily, when MDaemon receives mail that is intended for one of its gateways, it will store the mail until that domain connects to MDaemon to collect it. In some situations you may want MDaemon to attempt to deliver the mail directly via SMTP rather than waiting for the domain to collect it. When this option is enabled, MDaemon will attempt to deliver the domain's messages each time remote mail is processed. The gateway's mailbox will temporarily act as a remote queue and delivery will be attempted. Any messages that cannot be delivered will simply remain in the gateway's mailbox until they are collected by the domain or are successfully delivered later; they will not be moved into the remote queue or retry system. However, if you do not have the domain's DNS properly configured, or if you have your MDaemon configured to pass all outgoing messages to some other host for delivery, then you could cause those message to get caught in a mail loop and then eventually be treated as undeliverable.

Automatically extract embedded attachments
Some mail systems require attached files be extracted before submission of mail messages to the mail stream. To facilitate this, MDaemon can auto-extract incoming MIME attachments and place them in the `\Files\` subfolder underneath the domain's message folder. Check this box if you wish to automatically extract attachments.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.3.3.2 Verification



One common problem with domain gateways and mail-drops is that they don't usually have a method for determining whether or not the recipient of an incoming message is valid. For instance, if you act as a gateway for `example.com` and a message comes for `user01@example.com` then you have no way of knowing whether or not there is actually a mailbox, alias, or mailing list corresponding to that address on example.com's email server. Thus you have no choice but to assume that the address is valid and accept the message. Further, since spammers commonly send messages to many invalid addresses, this problem can result in large amounts of junk email be accepted for the gateway.

MDaemon contains a method to prevent this by verifying the recipient addresses. If the remote domain's server is configured to keep an LDAP or Active Directory server up to date with all of its mailboxes, aliases, and mailing lists, or if it runs a Minger server to provide remote address verification, then you can use the options on this screen to specify the LDAP, Active Directory, or Minger server where this information is stored. Then, when a message arrives for `example.com`, you can lookup the recipient's address on the other server and discover whether or not it is valid.

Address Verification

Verify addresses using:

Nothing
Choose this option if you do not wish to use email address verification for this domain gateway. MDaemon will treat all of the domain's incoming messages as if

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

the recipient is a valid address, since it will have no way of identifying which addresses actually exist for that domain.

File
Choose this option if you wish to use the `GatewayUsers.dat` file as the definitive list of addresses that will be used to verify whether or not the recipient of an incoming message for this domain is valid. This is a global list of addresses, applicable to all of your domain gateways, and even if you have chosen to use one of the other verification methods, this list will still be used as an extra source of valid addresses. When using the *File* option, however, it will be the only verification option used. You can open and edit the valid address list by clicking the *Address verification file* button below.

LDAP
Choose this option to activate remote address verification via LDAP or Active Directory. Whenever a message arrives for the remote domain its LDAP or Active Directory server will be queried to determine whether or not the recipient is valid. If it isn't valid the message will be rejected. If MDaemon is unable to connect to the LDAP/AD server then it will assume the address is valid.

Minger
Choose this option if you wish to query the domain's Minger server to verify recipient addresses for this domain. If MDaemon is unable to connect to the server then it will assume the address is valid. There is also a global option located on Global Gateway Settings 165 that you can use to cause MDaemon to query your Domain Sharing 75 hosts as well.

Host name or IP
Enter the host name or IP address of the domain's LDAP/Active Directory or Minger server. This is the LDAP/AD or Minger server to which MDaemon will connect in order to verify that the recipient of an incoming message is a valid address at the domain for which this MDaemon is acting as a gateway or backup server.

Port
Specify the port that the domain's LDAP/AD or Minger server is using. MDaemon will use this port when verifying address information via LDAP, Active Directory, or Minger.

Test
Click this button to test whether or not you have the remote address verification settings configured properly. MDaemon will simply attempt to connect to the designated LDAP/AD server and verify that it responds to the specified information.

Cache
Click this button to open the LDAP/Minger cache. You can enable/disable the cache on Global Gateway Settings 165.

User name or Bind DN
Enter the User name or DN of the account that has administrative access to the domain's LDAP/AD server so that MDaemon can verify the recipients of incoming messages addressed to the domain for which it is acting as a gateway or backup

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

server. This is the DN used for authentication in the bind operation.

Password or Minger shared secret
This password will be passed to the domain's LDAP/AD server along with the *Bind DN* value for authentication. If using a Minger server then this is the shared secret or password used.

Base entry DN
This is the Distinguished Name (DN) or starting point in the Directory Information Tree (DIT) at which MDaemon will query your LDAP/AD server for address verification.

Search filter
This is the LDAP/AD search filter that will be used when querying your server to verify addresses. MDaemon will setup a default search filter that should work in most cases.

Search scope:

This is the scope or extent of your LDAP/AD searches.

Base DN only
Choose this option if you wish to limit your search to only the base DN specified above. The search will not proceed below that point in your tree (DIT).

1 level below base DN
Use this option if you wish to extend your LDAP/AD search to one level below the supplied DN in your DIT.

Base DN and all children
This option will extend the scope of your search from the supplied DN to all of its children, down to the lowest child entry in your DIT.

Address verification file
Click this button to open the Gateway Valid Email Address List (i.e. the `GatewayUsers.dat` file). This contains a list of addresses that MDaemon will consider to be valid recipients for incoming messages addressed to your domain gateways. Regardless of the verification option selected above, MDaemon will use this list as an extra source of valid address data. When using the *File* option above, however, it will be the definitive and only verification option used.

Using multiple configurations for LDAP verification queries

You can specify multiple LDAP configurations for your gateway domains. To specify extra sets of LDAP parameters, setup your first set normally and then manually edit the `GATEWAYS.DAT` file using Notepad.

Your new set of parameters should be created using the following format:

```
LDAPHost1=<host name>
LDAPPort1=<port>
LDAPBaseEntry1=<base entry DN>
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

```
LDAPRootDN1=<root DN>
LDAPObjectClass1=USER
LDAPRootPass1=<password>
LDAPMailAttribute1=mail
```

For each new set of parameters, increase the numeral in each parameter's name by 1. For example, in the sample set above, each parameter's name ends with "1". To create an additional set each name would end with "2". In another set, each would end "3", and so on.

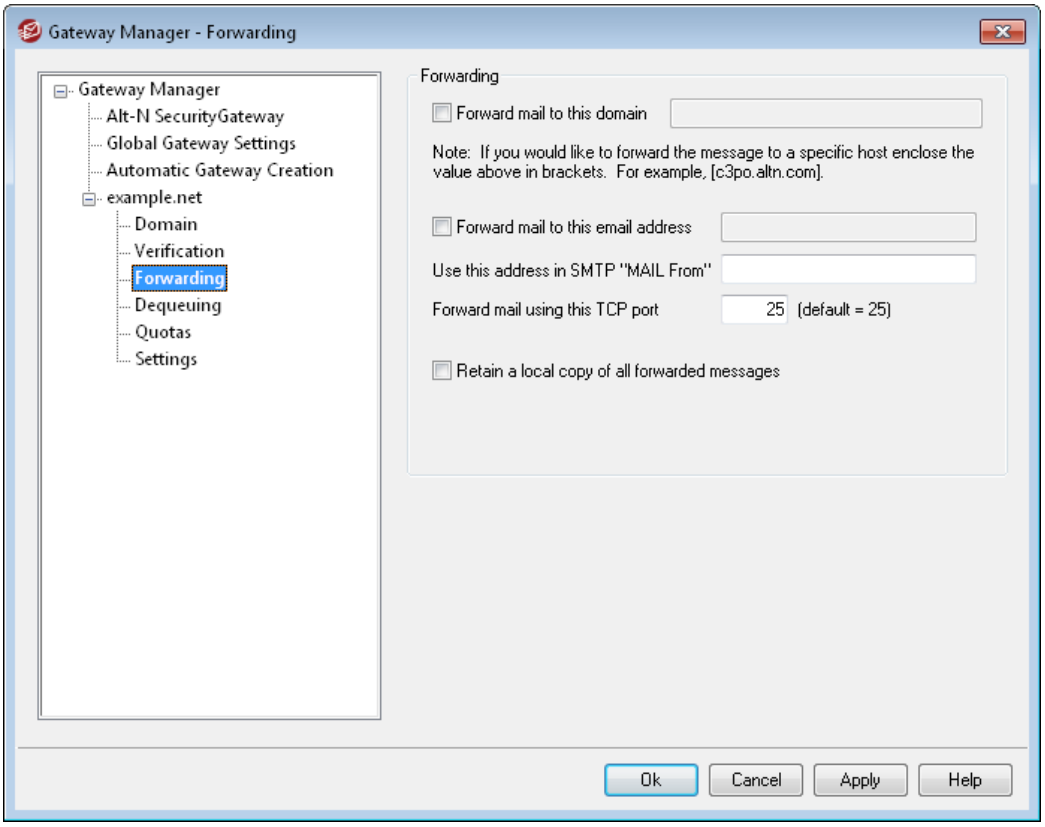
When the LDAP queries take place, MDaemon will perform multiple LDAP queries in sequence to find a match. If an error or a match is found no further checks are performed.

See:

LDAP/Address Book Options 105
Minger 640

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.3.3.3 Forwarding



Forwarding

Forward mail to this domain
Sometimes it is advantageous to simply forward a copy of all messages for a domain as they arrive. If you wish to configure MDaemon to do this, enter the name or IP address of the domain to which copies of incoming mail for this domain should be sent. If you wish to forward the messages to a specific host then place the value in brackets (for example, `[host1.example.net]`).

Forward mail to this email address
Use this feature if you wish to forward to a specific email address all email messages destined for this client domain.

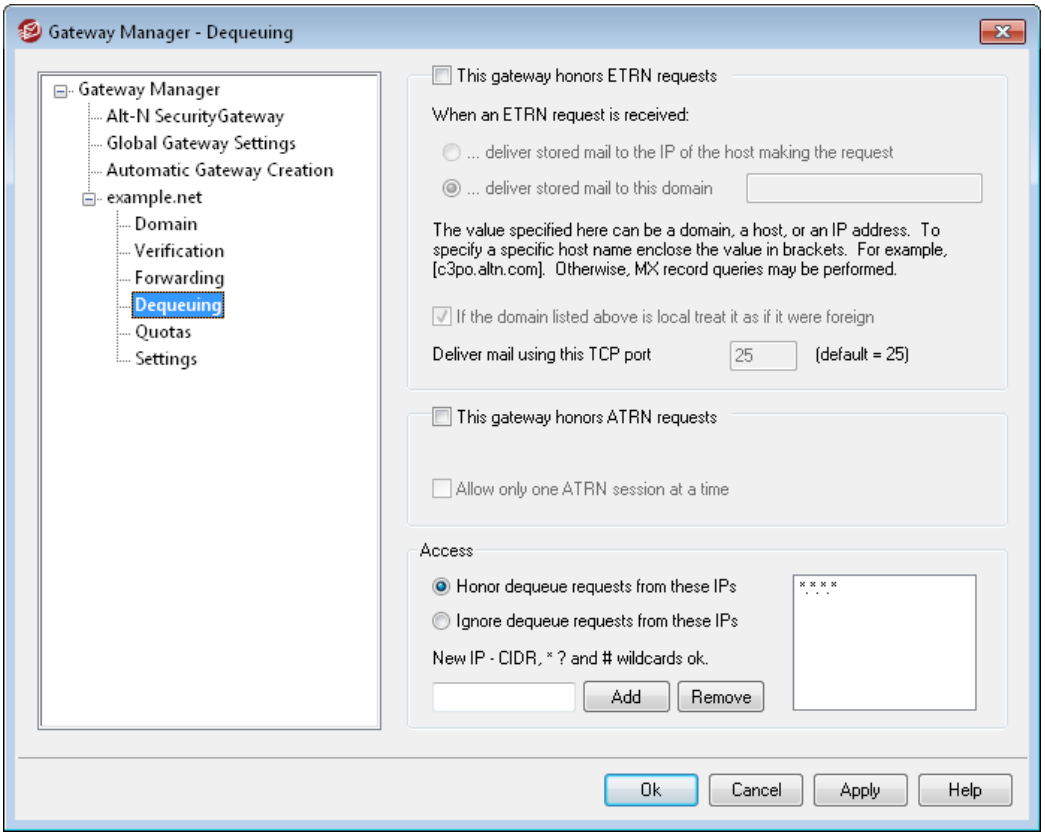
Use this address in SMTP "MAIL From"
MDaemon will use this address in the SMTP "Mail From" transaction.

Forward mail using this TCP port
MDaemon will forward this mail using this TCP port.

Retain a local copy of all forwarded messages
Select this option if you wish MDaemon to retain an archival copy of each message locally once it has been forwarded.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.3.3.4 Dequeuing


Gateway Manager - Dequeuing
Gateway Manager
Alt-N SecurityGateway
Global Gateway Settings
Automatic Gateway Creation
example.net
Domain
Verification
Forwarding
Dequeuing
Quotas
Settings
This gateway honors ETRN requests
When an ETRN request is received:
... deliver stored mail to the IP of the host making the request
... deliver stored mail to this domain
The value specified here can be a domain, a host, or an IP address. To specify a specific host name enclose the value in brackets. For example, [c3po.altn.com]. Otherwise, MX record queries may be performed.
If the domain listed above is local treat it as if it were foreign
Deliver mail using this TCP port
25
(default = 25)
This gateway honors ATRN requests
Allow only one ATRN session at a time
Access
Honor dequeue requests from these IPs
Ignore dequeue requests from these IPs
New IP - CIDR, * ? and # wildcards ok.
Add
Remove
..*.*
Ok
Cancel
Apply
Help

ETRN

This gateway honors ETRN requests
When this switch is enabled MDaemon will respond to ETRN requests made by qualified hosts on behalf of the domain for which MDaemon is acting as an email gateway. The ETRN command is an SMTP extension that signals a server storing mail for a particular domain that it is time to begin spooling the mail. When MDaemon receives an ETRN request for a domain, it will immediately begin spooling the stored mail for delivery using subsequent SMTP transactions. Please note that the SMTP session that issues an ETRN request will not be the one that receives any stored mail. MDaemon will use subsequent independent SMTP transactions to send any mail it has stored for the domain. This preserves the message envelope and is more secure. Also note that the host to which MDaemon will spool any stored mail may not immediately begin reception of these messages. ETRN only guarantees that any stored mail is *spooled* for delivery. The actual *process* of delivery is subject to other administrator-imposed restrictions and may have to wait in the outbound mail queue for the next scheduled remote mail processing event to take place. Because of these limitations we recommend using On-Demand Mail Relay (ODMR) 68 and its ATRN command rather than ETRN. This method is not supported by all clients and servers, however, and will therefore only be available to client domains using a server that does so. MDaemon fully supports ODMR on both the client and server side.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

By default MDaemon requires that the connecting host issuing the ETRN request first authenticate itself via ESMTP AUTH using the *Domain name* 168 and *Gateway AUTH password* 179 as its login credentials. If you do not wish to require authentication than you can disable it on Settings 179 by clearing *ETRN dequeuing requires authentication*.

When an ETRN request is received:

...deliver stored mail to the IP of the host making the request
Selecting this option will cause MDaemon to send any stored mail to the IP address of the machine that made the ETRN request. The requesting machine must be running an SMTP server to receive these messages.

...deliver stored mail to this domain
This is the host name, domain name, or IP address to which any stored mail will be sent when an ETRN request is received and honored. The receiving machine must be running an SMTP server to receive these messages. Note: when a domain name is specified in this option, A and MX records may be used, depending on the DNS results during delivery. If you wish to deliver the messages to a particular host then place the host name in brackets (for example, `[host1.example.net]`) or specify an IP address instead of a domain name.

If the domain listed above is local treat it as if it were foreign
Activate this control if the domain is local but you want its mail to be spooled as if it is remote.

Deliver mail using this TCP port
Use this box to specify the port on which the domain's mail will be spooled.

ATRN

This gateway honors ATRN requests
Enable this option if you want MDaemon to respond to `ATRN` commands from the gateway's domain. `ATRN` is an ESMTP command used in On-Demand Mail Relay (ODMR) 68, which is currently the best relay method available for mail hosting. It is superior to ETRN and other methods in that in requires authentication before mail is dequeued and does not require a static IP address. A static IP address isn't required because the flow of data between MDaemon and the client domain is immediately reversed and the messages are de-spooled without having to make a new connection, unlike `ETRN`, which uses a separate connection after the `ETRN` command is sent. This enables client domains with a dynamic (non-static) IP address to collect their messages without having to use POP3 or DomainPOP, because the original SMTP envelope is preserved.

ATRN requires a session using the AUTH command. You can configure the authentication credentials on the Settings 179 screen.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Allow only one ATRN session at a time
Click this check box if you wish to restrict ATRN to one session at a time.

Access

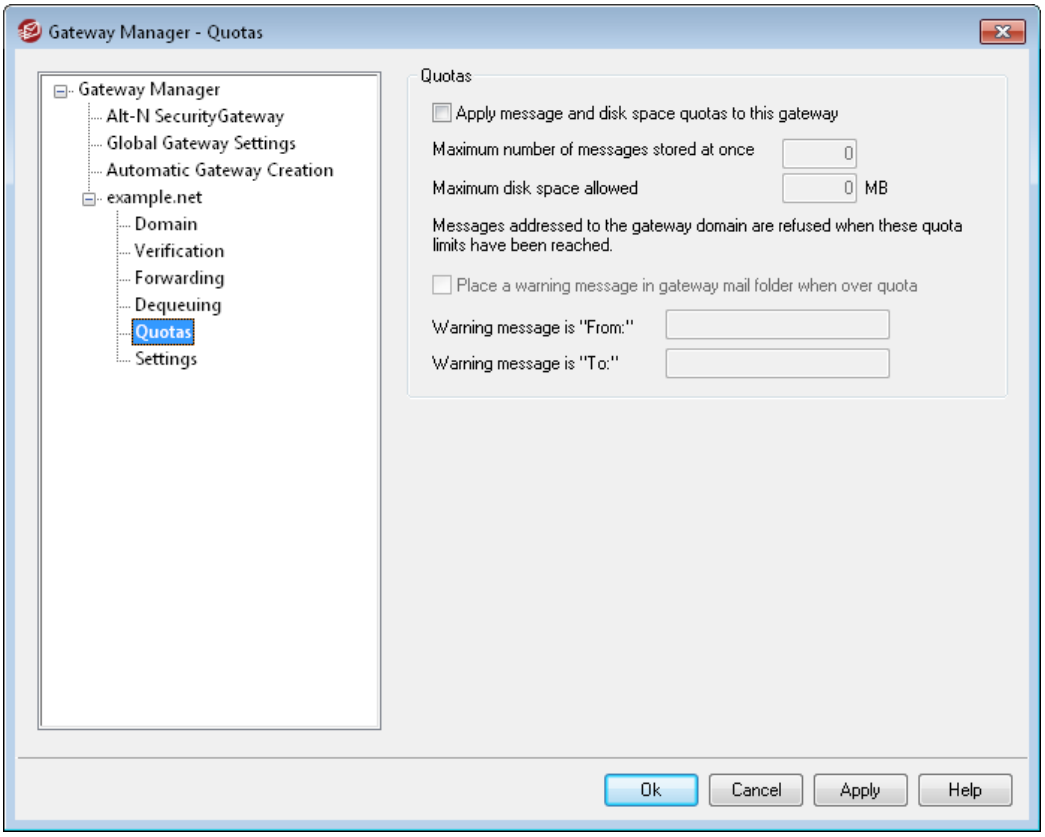
Honor dequeue requests from these IPs
Select this switch and MDaemon will honor ETRN/ATRN requests made from any IP listed in the associated address list.

Ignore dequeue requests from these IPs
Select this switch and MDaemon will ignore ETRN/ATRN requests that are made from any IP listed in the associated address list.

Add new IP
To add a New IP to the current list simply enter the IP into this text box and click the *Add* button.

Remove
Click this button to remove a selected entry from the list of IP addresses.

3.3.3.5 Quotas



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Quotas

Apply message and disk space quotas to this gateway
Enable this option if you wish to designate a maximum number of messages allowed to be stored for the domain or a maximum amount of disk space (in kilobytes) that it can use. This includes any decoded file attachments in its Files directory. When a quota is reached, any further incoming messages addressed to the domain will be refused.

Maximum number of messages stored at once
Use this box to designate the maximum number of messages that MDaemon will store for this gateway domain. Use "0" in this option if you do not wish to limit the number of messages.

Maximum disk space allowed
Specify the maximum allowed disk space here. When messages and files stored for the domain reach this limit, any further incoming messages for the domain will be refused. Use "0" if you do not wish to set a disk space limit.

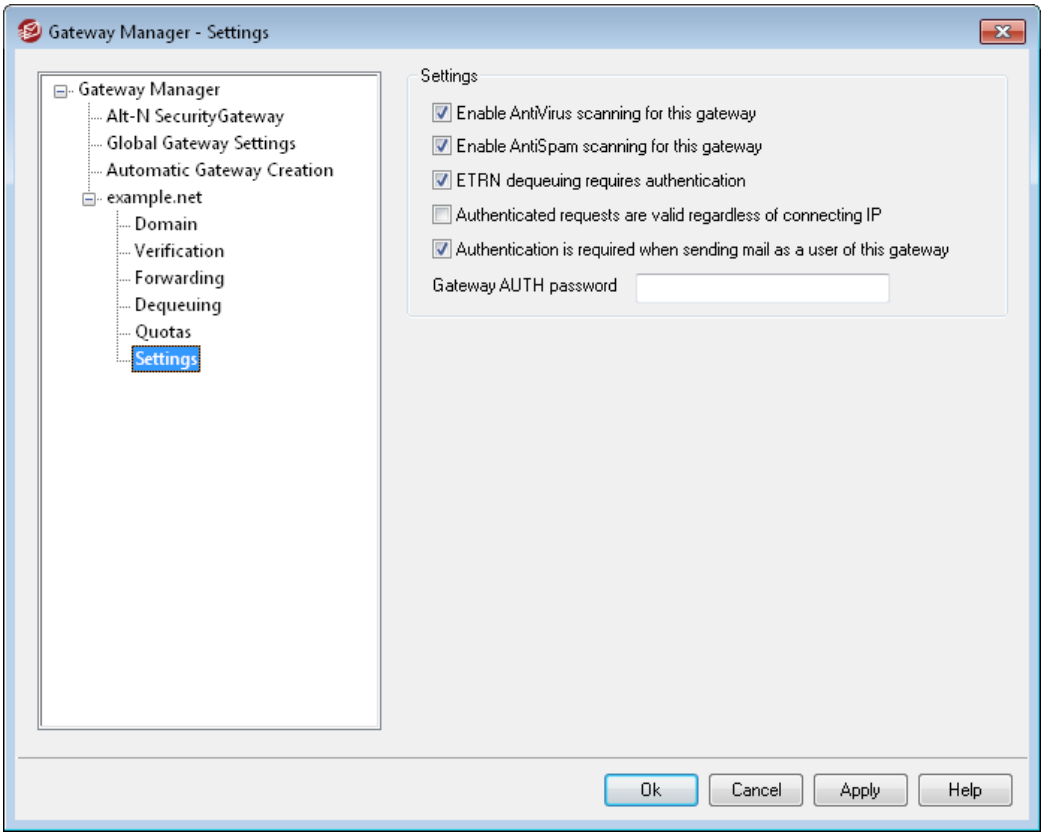
Place a warning message in gateway mail folder when over quota
If this option is enabled and a mail delivery to the domain is attempted that would exceed the maximum message or disk space limitations, an appropriate warning message will be placed in the domain gateway's mail folder. You can designate the warning message's "`From:`" and "`To:`" headers below.

Warning message is "From:"
Use this option to specify the "From:" address that will be used in the over-quota warning messages.

Warning message is "To:"
Use this option to specify the "To:" address that will be used in the over-quota warning messages.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.3.3.6 Settings



Settings

Enable AntiVirus scanning for this gateway
Click this option if you have installed SecurityPlus for MDaemon and want this domain gateway's messages to be scanned. If you clear this option then SecurityPlus will not scan this gateway's messages.

Enable AntiSpam scanning for this gateway
Click this option if you want to apply the Spam Filter settings to this domain gateway's messages. Otherwise, they will be excluded from Spam Filter scanning.

ETRN dequeuing requires authentication
When you configure the settings on the Dequeuing tab to accept ESMTP ETRN requests, this option will be used by default to require the connecting host to first authenticate using the ESMTP AUTH command. When this option is enabled, you must designate an authentication password in the "Auth password" box provided below.

Clear this checkbox if you do not wish to require authentication of hosts making ETRN requests.

Authenticated requests are valid regardless of connecting IP
Enable this checkbox if you wish to honor authenticated requests regardless of the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

IP address from which they are coming. If this control is not enabled then only requests from those IP addresses specified in the Access section will be honored.

Authenticated is required when sending mail as a user of this gateway
Click this check box if you want all messages claiming to be from this domain to require authentication. If a message is purported to be from this domain then it must be using an authenticated connection (or connecting from a Trusted IP address) or it will be refused. This option is enabled by default.

When new domain gateways are created, this option will be enabled by default. If you wish to change the default setting so that new gateways will have this option disabled, then edit the following key in the `MDaemon.ini` file:

```
[Special]
GatewaySendersMustAuth=No (default is Yes)
```

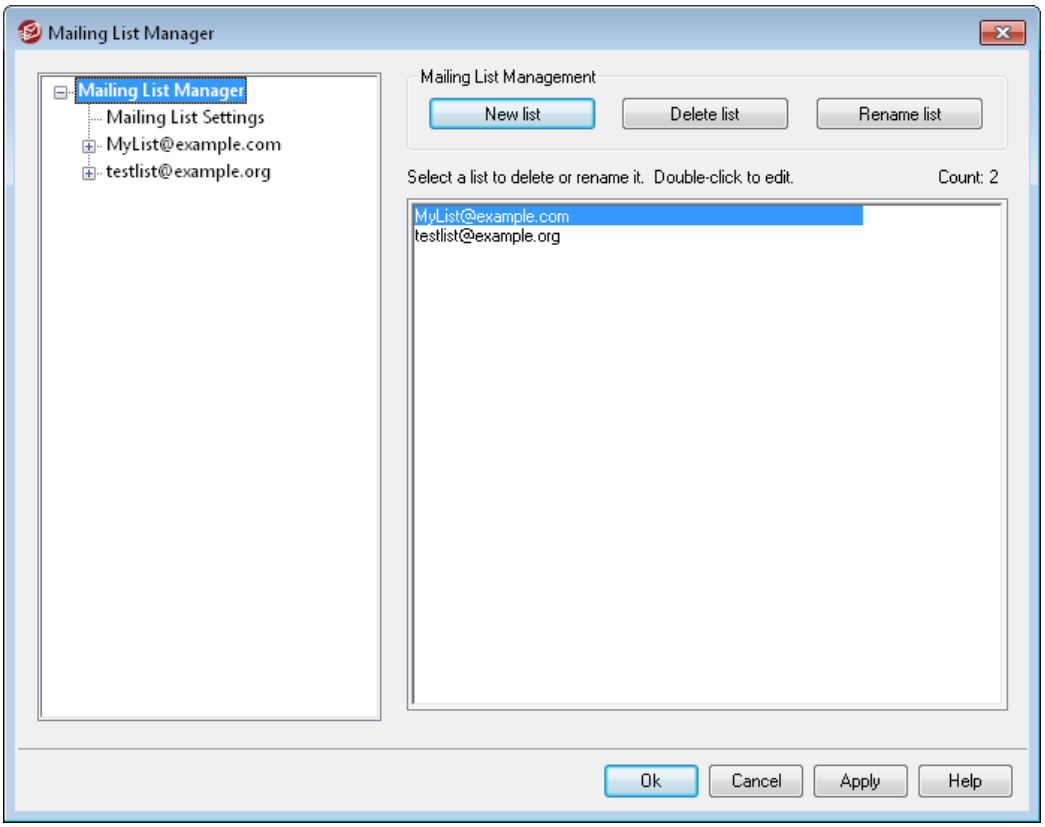
Gateway AUTH password
When using ATRN to dequeue this gateway's mail, or when you are requiring authentication via the *ETRN dequeuing requires authentication* option above, designate the gateway's AUTH password here.

The domain for which MDaemon is acting as an email gateway must use its domain name as the logon parameter. For example, if the domain gateway is "example.com" and is using ATRN to dequeue its mail, then it would authenticate using the login credentials "example.com" and the password specified here.

3.4 Mailing List Manager

Mailing Lists, sometimes called Email Groups or Distribution Lists, allow groups of users to be addressed as if they all shared a common mailbox. Copies of email messages sent to the list are distributed to each of the list's members. Lists may contain members with local and/or remote destination addresses, be public or private, moderated or open, be sent in digest 199 or normal message format, and more.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Located under the Setup » Mailing List Manager... menu selection, the Mailing List Manager is used to administer your lists.

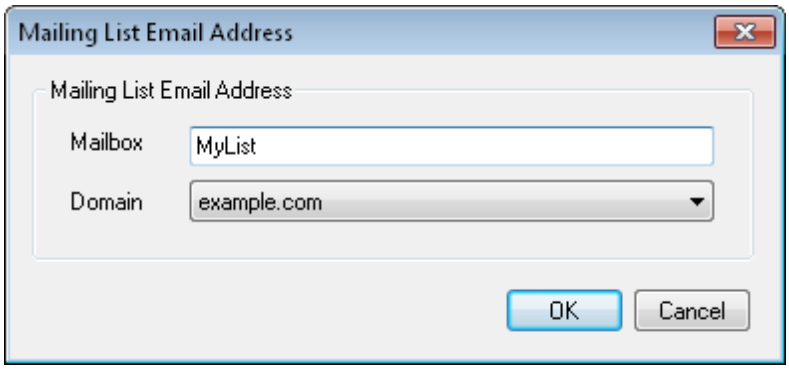
Mailing List Management

The navigation pane on the left side of this dialog contains an entry for each of your mailing lists, with links to each screen used for configuring the various list-specific settings. It also provides access to the Mailing List Settings 183 screen, which is used for configuring several list-related global options. The options on the right side of this dialog are used for creating, deleting, and renaming your lists. You can double-click a mailing list to switch to the mailing list editor for configuring the list's settings.

New list

To create a new mailing list, click **New list** to open the Mailing List Email Address dialog. Create a mailbox name and select a domain, such as "MyList" and "example.com" respectively. This will be the mailing list's email address (i.e. MyList@example.com). Messages sent to this address will be distributed to members of the list, based on the list's particular settings. Click **OK** to create the list. After creating the list you can double-click its entry to configure its settings and add members. **Note:** List names cannot contain " ! " or " | "

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Delete list
To delete a mailing list: select the list, click **Delete list**, and click **Yes** to confirm your decision.

Rename list
To rename a mailing list, select the list and then click **Rename list** to open the Mailing List Email Address dialog. Make your desired changes and click **OK**.

Modifying an Existing Mailing List

To configure a mailing list, double-click its entry on the Mailing List Manager. Then in the navigation pane on the left, click whichever screen you wish to edit:

Members 186
Settings 189
Headers 192
Subscription 194
Reminders 198
Moderation 202
Digest 199
Routing 204
Notifications 201
Support Files 206
Public Folder 208
Active Directory 209
ODBC 211

Mailing List Settings

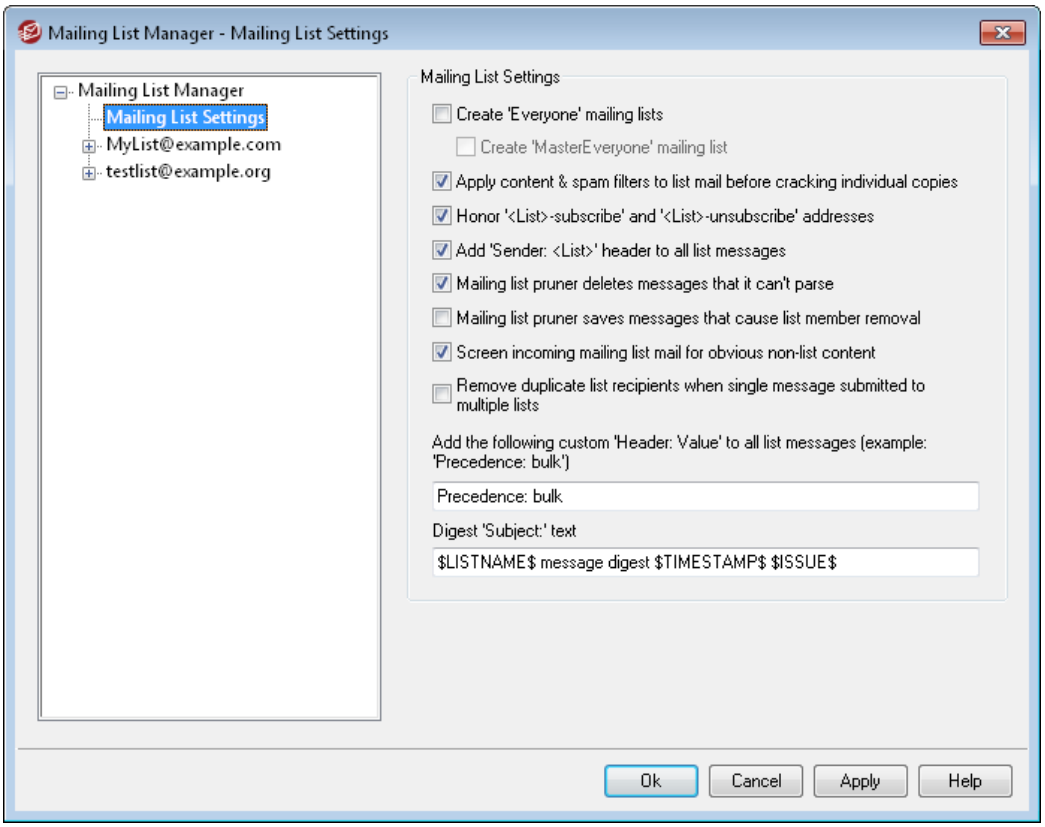
Click **Mailing List Settings** in the left pane to open the Mailing List Settings 183 screen, for configuring several global settings related to mailing lists.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Mailing List Settings 183

3.4.1 Mailing List Settings


Mailing List Manager - Mailing List Settings
Mailing List Manager
Mailing List Settings
MyList@example.com
testlist@example.org
Mailing List Settings
Create 'Everyone' mailing lists
Create 'MasterEveryone' mailing list
Apply content & spam filters to list mail before cracking individual copies
Honor '<List>-subscribe' and '<List>-unsubscribe' addresses
Add 'Sender: <List>' header to all list messages
Mailing list pruner deletes messages that it can't parse
Mailing list pruner saves messages that cause list member removal
Screen incoming mailing list mail for obvious non-list content
Remove duplicate list recipients when single message submitted to multiple lists
Add the following custom 'Header: Value' to all list messages (example: 'Precedence: bulk')
Precedence: bulk
Digest 'Subject:' text
$LISTNAME$ message digest $TIMESTAMP$ $ISSUE$
Ok
Cancel
Apply
Help

Mailing List Settings

Create "Everyone" mailing lists
Check this box if you wish to create and maintain "Everyone" mailing lists for all of your domains (e.g. "everyone@example.com"). A list will be created for each domain, which makes it possible for you to send a message to every user of a domain simply by addressing the message to "everyone@<domain>". Private accounts 573 are hidden from "Everyone" mailing lists. This option is disabled by default.

Create "MasterEveryone" list
Enable this option if you want there to be a "MasterEveryone" mailing list. Everyone on all of your domain-specific "everyone" lists will be included on this list. This option is disabled by default.

Apply content & spam filters to list mail before cracking individual copies
When the *Deliver list mail to each member individually* option is chosen on the Routing 204 screen of the mailing list editor, enabling this control will cause the content filter

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

rules and spam filter to be applied to list messages before they are copied and distributed to list members.

Honor '<List>-subscribe' and '<List>-unsubscribe' addresses
Click this checkbox if you want MDaemon to recognize email addresses of this format as valid (as long as the list actually exists) in order to facilitate an easier method for users to join and leave your mailing lists. For example: suppose you have a list called `MyList@example.com`. People will be able to subscribe/unsubscribe to your list by sending an email message to `MyList-Subscribe@example.com` and `MyList-Unsubscribe@example.com`. The content of the subject and message body is irrelevant. Also, when this feature is active MDaemon will insert the following header into all list messages:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

Some mail clients can pick up on this and make an UNSUBSCRIBE button available to users automatically.

You can override this option for individual lists by specifying a value for the List-Subscribe and List-Unsubscribe headers in the **Mailing List URLs** options located on the Mailing List Editor's Moderation 202 screen.

Add 'Sender: <List>' header to all list messages
Enable this option if you wish to insert the `Sender` header into mailing list messages.

Mailing list pruner deletes messages that it can't parse
When this option is enabled, MDaemon will delete list messages that do not contain a parsable address.

Mailing list pruner saves messages that cause list member removal
When MDaemon scans returned list messages in an attempt to remove member addresses that cannot be reached, this control will cause messages that result in a list member's removal to be saved. For more information, see the *Remove undeliverable email addresses...* option on the Settings 189 screen.

Screen incoming mailing list mail for obvious non-list content
Check this box if you wish MDaemon to reject messages addressed to a mailing list when it determines that they should have been addressed to the system account instead. For example, a user may join or leave a list by placing the Subscribe or Unsubscribe command at the beginning of an email message and sending that message to the system address (e.g. "mdaemon@example.com"). Oftentimes users erroneously try to send those sorts of messages to the list itself. This option will prevent those messages from being posted to the list.

Remove duplicate list recipients when single message submitted to multiple lists
When this option is enabled and a single message is addressed to multiple mailing lists, MDaemon will deliver only one copy of the message to any recipient who is a member 186 of more than one of the lists. For example, if `frank@example.net` is a

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

member of `List-A@example.com` and `List-B@example.com` and an incoming message is addressed to both lists, Frank will receive only one copy of the message rather than two. This option only applies to lists, therefore in the above example if the message were addressed to Frank directly, plus the two lists, then Frank would receive two copies of the message rather than three. This option is disabled by default.

Using this option is not generally recommended. Mailing lists can be used and organized many different ways by users, and there is no way of knowing which list will receive the message when limiting duplicates in this way. Therefore using this option could cause unnecessary difficulties for some users, due to message threading preferences, using IMAP filters 541 to sort messages to specific folders, and so on.

Add the following custom 'Header: value' to all list messages
If you wish to add a static header/value combination (such as "Precedence: bulk") to all list messages, specify that text here.

Digest 'Subject:' text:
Use this option if you wish to customize the subject used when MDaemon sends mailing list digest 199 messages. The default is: "`$LISTNAME$ message digest $TIMESTAMP$ $ISSUE$.`" The macros expand to the name of the mailing list, the time-stamp of the digest message creation, and the issue number.

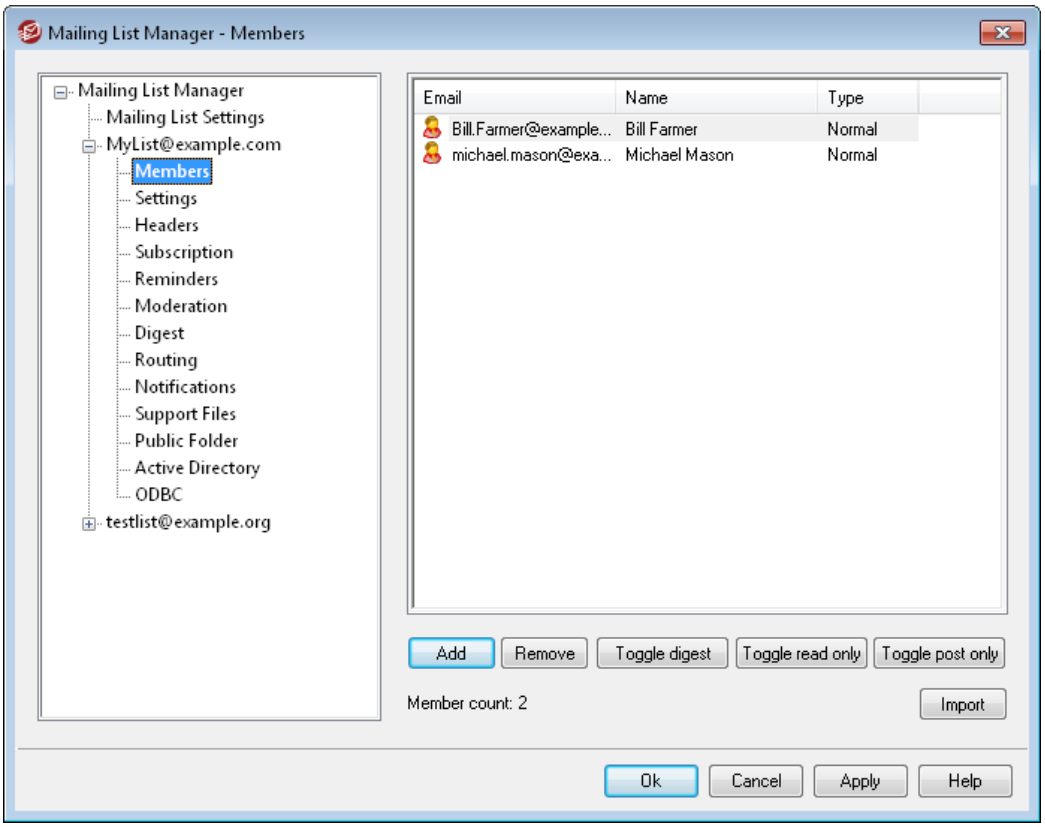
See:

Mailing List Manager 180

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.4.2 Mailing List Editor

3.4.2.1 Members



This screen displays the email addresses and names of all members currently subscribed to the list. Each member's entry also states its "type" of membership: normal, digest, read only, or post only. To edit a member's settings, double-click the member's entry.

Add
This button opens the New List Member screen for adding new members 187.

Remove
To remove a member from the list, select its entry and then click this button.

Toggle digest
Select a member and then click this button to make it a Digest 199 membership. Click the button again to return the member to "normal" mode.

Toggle read only
Select a member's entry and then click this button to switch it to "Read Only" mode. The member will still receive messages from the list but will not be allowed to send them to it. Click the button again to return the member to "normal" mode.

Toggle post only
Clicking this button after selecting a member will set the membership to "Post Only."

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

A Post Only member can send messages to the list but will not receive any. Click the button again to return the member to "normal" mode.

Import
Click this button to import list members from a text file that has its fields separated by commas (i.e. a comma delimited file). Each entry must be on its own line and all of its fields must be separated by commas. Further, the first line of the file (the baseline) must list the names of the fields and the order in which they appear in the remaining lines. One of the fields must be called "**Email**" and contain email addresses. There are also two optional fields: "**FullName**" and "**Type**". FullName is for the list member's name. Type can have a value of: "read only", "post only", "digest", or "normal". All other fields will be ignored by the importer.

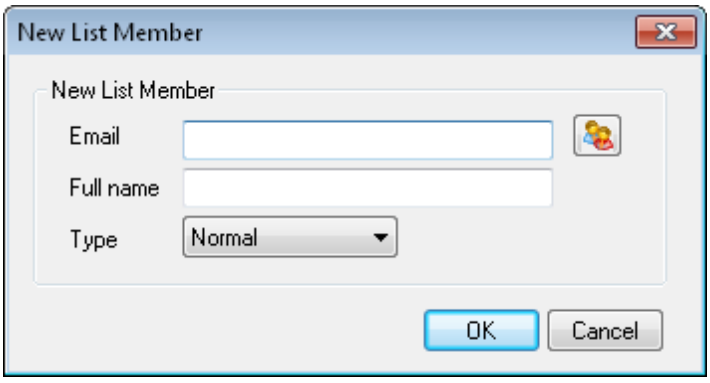
For example:

```
"Email", "FullName", "Type", "Address", "telephone"
"user01@altn.com", "Michael Mason", "Digest", "123 Street St",
"519.555.0100"
```

Imported members do not receive the list welcome packet (if any), and the importer will not check for member duplicates.

Member count:
The total number of members currently subscribed to the list is displayed at the bottom of the screen.

Adding New Members



New List Member

Email
Enter the email address that you wish to add to the mailing list, or click the Account icon if you wish to browse MDaemon accounts to add one to the list. List member addresses cannot contain " ! " or "|".

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

If you wish to add all of your MDaemon users, all users of one of your domains, or all users belonging to a specific group, you can enter `ALL_USERS`, `ALL_USERS:<domain>`, or `GROUP:<group-name>` respectively, instead of entering a specific email address. For example, adding `ALL_USERS:example.com` as a member of a list has the same effect as adding every `example.com` user account separately. Adding `ALL_USERS` as a member is the same as added every MDaemon account, regardless of the domain.

Full name
Enter the member's name in this field. This name will appear in the "To:" header of list messages when the "*Replace 'TO:' header 'Display Name' with Member's name*" option is selected on the Headers 192 screen.

Type
Use the drop-down box to choose the type of membership for the user:

Normal—The member can send and receive list messages normally.

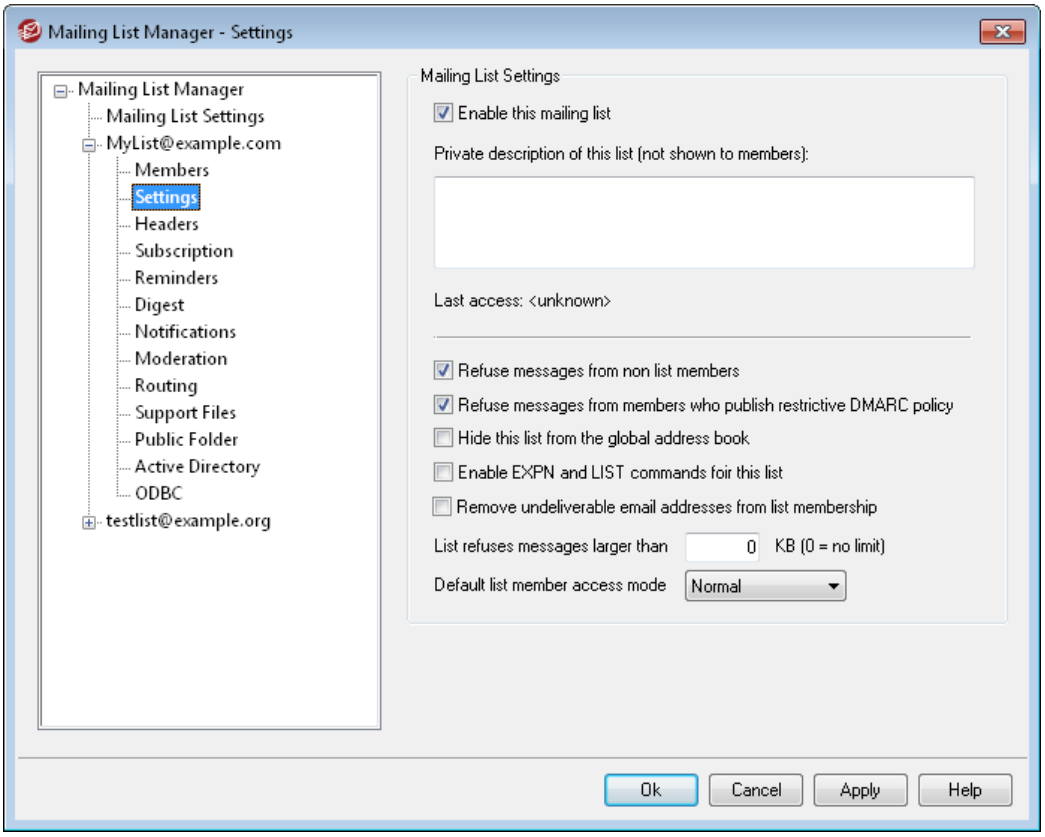
Digest—The member can send and receive list messages, but received messages will be in digest format.

Read only—The member will receive messages from the list but cannot send messages to it.

Post only—The list member can send messages to the list but will not receive them.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.4.2.2 Settings



Mailing List Settings

Enable this mailing list
Clear this checkbox if you wish to disable the mailing list temporarily. While the list is disabled, any message arriving via SMTP either to or from the list will generate a 451 temporary error and be refused.

Private description of this list (not shown to members)
You may enter a private description of the list here. This is for your own reference and it will not be displayed to any members or in any headers.

Last Access
Displays the time that someone last accessed this list. This can help you more easily identify lists that are rarely or no longer used.

Refuse messages from non list members
When this control is enabled, the list will be considered a "private" list, meaning that only list members can send messages to the list. Messages originating from non-members will be refused.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Refuse messages from domains with restrictive DMARC policies
Enable this option if you wish to reject any incoming message to the list that is sent by someone from a domain that publishes restrictive DMARC[455] policies (i.e. p=quarantine or p=reject). It is generally not necessary to enable this option if you are using the "*Replace 'From:' email address with list's email address if...*" option located on the Headers[192] screen.

If both this option and the "*Replace 'From:' email address with list's email address if...*[192]" option are disabled then that would likely cause some list messages to be rejected by some receiving servers, and in some cases it could cause the recipient to be automatically removed from list membership[191]. You should therefore take care to ensure that at least one of these options is enabled.

Hide this list from the global address book
Click this option to hide the mailing list from the WorldClient and LDAP public address books.

Enable EXPN and LIST commands for this list
By default MDaemon will not honor EXPN and LIST commands for lists, in order to keep the membership private. If you enable this option then the membership of the list will be reported in response to an EXPN or LISTS command during a mail session.

Remove undeliverable email addresses from list membership
When this feature is enabled, MDaemon will automatically remove an address from the members list when it encounters a permanent fatal error while attempting delivery. An addresses is also removed when the message is moved to the Retry[654] system and subsequently expires from that system.

The *Remove undeliverable email addresses...* option is only designed to assist in situations where the remote mail server refuses to accept messages. This will only work when "*Deliver list mail to each member individually*" has been selected on the Routing screen[204]. If you are instead routing list messages to a smart host then see Enhanced List Pruning[191] below for more information.

List refuses messages larger than [xx] KB
This control places an upper limit on the size of a message accepted for this mailing list. Messages larger than this limit are refused.

Default list member access mode
Use the drop-down list to set the default access mode to be used for for new members. You can change any existing member's access mode setting from the Members[186] screen. There are four membership modes:

Normal—The member can send and receive list messages normally.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Digest—The member can send and receive list messages, but received messages will be in digest format.

Read only—The member will receive messages from the list but cannot send messages to it.

Post only—The list member can send messages to the list but will not receive them.

Enhanced List Pruning

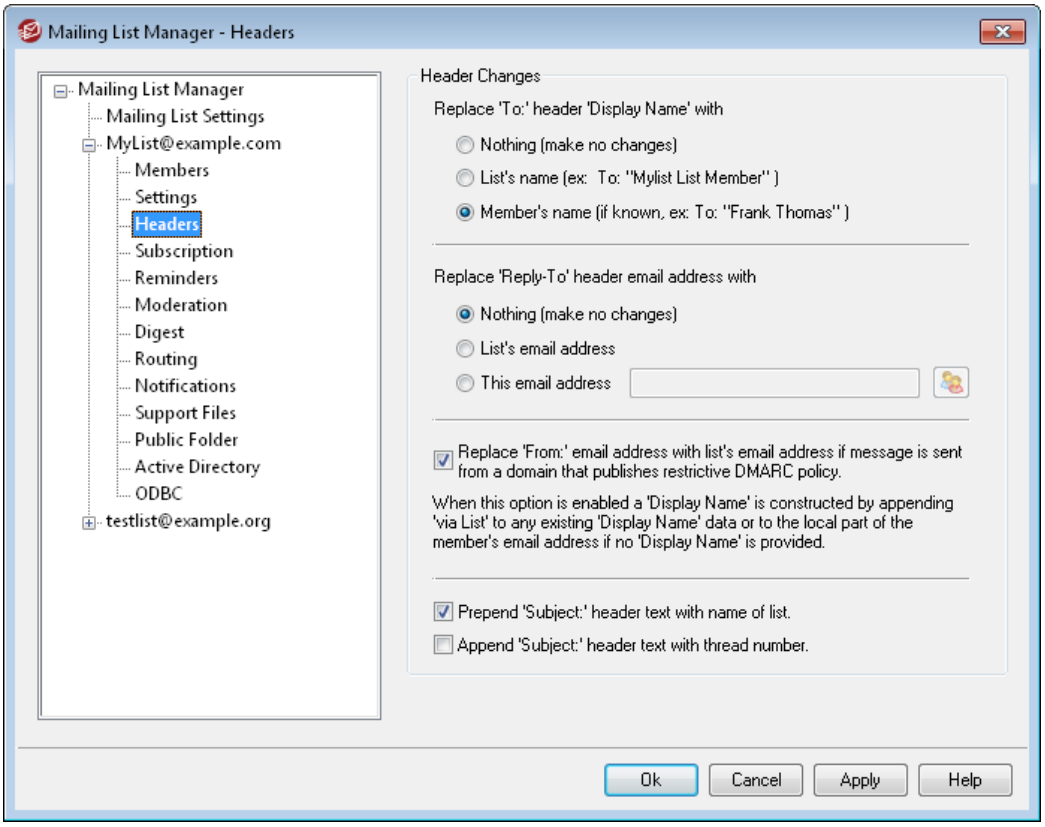
When the *Remove undeliverable email addresses from list membership* option is enabled and you have specified a local mailbox as the return path for the list's messages (see the *List's SMTP 'Bounce' address* option on Notifications 201), each day at midnight MDaemon will attempt to parse problem addresses from the returned mail and remove those members that couldn't be reached. This will aid in more efficiently pruning invalid addresses from mailing lists, especially when you are routing the list's messages to a smart host rather than delivering them directly.

On Mailing List Settings 183 there are two options related to this feature. The *Mailing list pruner deletes messages that it can't parse* option will cause returned messages that do not contain a parsable address to be deleted, and the *Mailing list pruner saves messages that cause list member removal* option will cause all messages that result in a list member being deleted to be saved.

Setting the *List's SMTP 'Bounce' address* 201 to a local user's address could cause that user's email to be deleted as a result of the list pruner settings designated on Mailing List Settings 183.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.4.2.3 Headers


Mailing List Manager - Headers
Mailing List Manager
Mailing List Settings
MyList@example.com
Members
Settings
Headers
Subscription
Reminders
Moderation
Digest
Routing
Notifications
Support Files
Public Folder
Active Directory
ODBC
testlist@example.org
Header Changes
Replace 'To:' header 'Display Name' with
Nothing (make no changes)
List's name (ex: To: "Mylist List Member")
Member's name (if known, ex: To: "Frank Thomas")
Replace 'Reply-To' header email address with
Nothing (make no changes)
List's email address
This email address
Replace 'From:' email address with list's email address if message is sent from a domain that publishes restrictive DMARC policy.
When this option is enabled a 'Display Name' is constructed by appending 'via List' to any existing 'Display Name' data or to the local part of the member's email address if no 'Display Name' is provided.
Prepend 'Subject:' header text with name of list.
Append 'Subject:' header text with thread number.
Ok
Cancel
Apply
Help

Header Changes

Replace 'TO:' header 'Display Name' with
Use this option to designate the text to display in the name portion of the TO: header whenever MDaemon receives a message directed to the list.

Nothing (make no changes) - When this options is selected MDaemon will make no changes. The display name and address contained in the TO: header will appear exactly as the sender of the message entered them.

List's name - This option replaces the displayed name with the name of the list plus "List Member". For example, for a mailing list named "My-Family" the display name portion of the To: header would say, "My-Family List Member".

Member's name (if known) - When this option is selected, the TO: header will contain the name (if available) and address of the list member to whom the message is directed.

The *Member's name* option can only be chosen when "*Deliver list mail to each member individually*" has been selected on the Routing screen 204. When "*Deliver list mail using individual RCPT commands for each member*" is selected, MDaemon will default to the *List's name* option.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Replace 'Reply-To:' header email address with
This option is for designating the email address that will appear in each list message's Reply-To: header.

Nothing (make no changes)
Choose this option if you wish to leave the Reply-To: header unchanged from whatever it is in the original message that will be distributed to the list. This is generally the option you should choose when you want replies to be directed back to whomever posted the message to the list, rather than to all of the list's members.

List's email address
Choose this option if you want replies to be directed to the list rather than to a specific person or address. This is the option you should choose if you wish to use the list as a group discussion tool, where replies are sent to all members.

This email address
If there is a specific email address to which you wish replies to be sent then type it here, or click the Account icon if you wish to browse for a specific MDaemon account to use. You could use this option, for example, for something like an email newsletter with a specific contact address for replies.

Replace 'From:' email address with list's email address if message is sent from a domain that publishes restrictive DMARC policy
By default, when an incoming message to the list is sent from a user at a domain that publishes a restrictive DMARC 455 policy (i.e. p=quarantine or p=reject), MDaemon will replace the user's email address in the From: header with the address of the list, before sending the message to the list. This is necessary to prevent the list message from being rejected by servers that honor restrictive DMARC policies. In addition to changing the From: header's email address, the displayed name will also be modified to add "via List Name," to show that it is a message sent by that mailing list on behalf of the named person. Further, any time the From: header is changed by this feature the original From: header data will be moved into the Reply-To: header, but only if the message has no Reply-To: header to begin with and the list isn't configured to display a custom Reply-To: header.

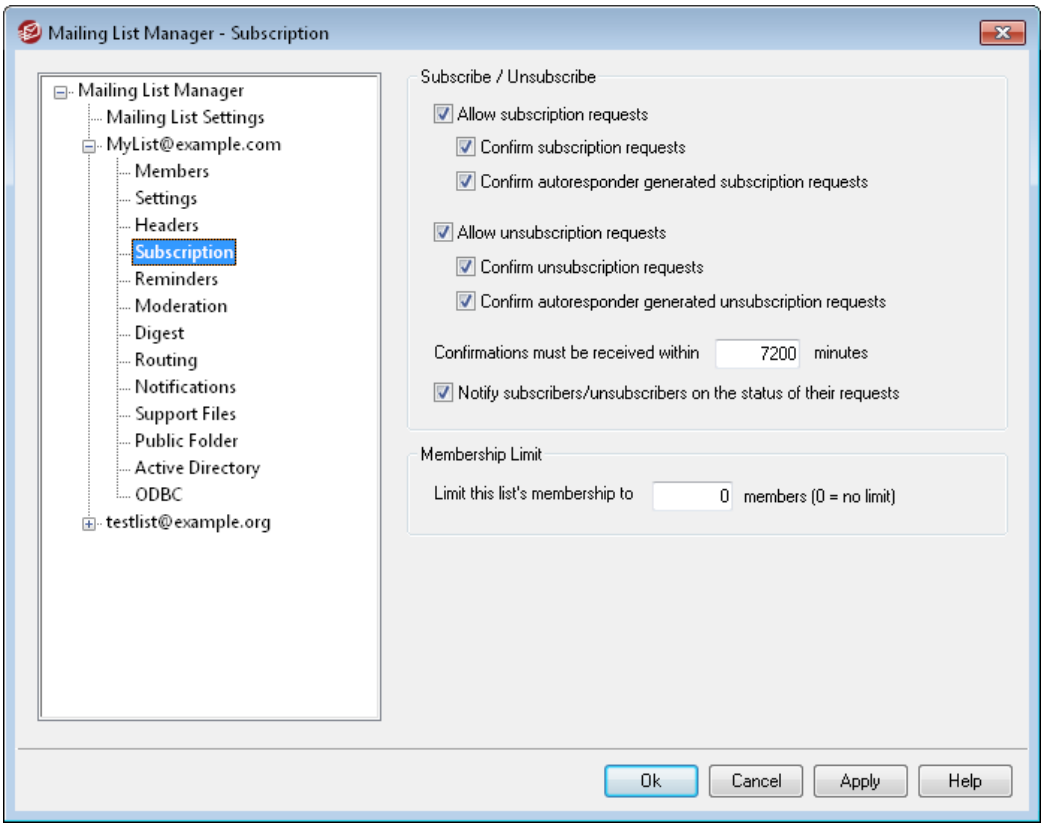
You should not disable this option unless you fully understand the ramifications of doing so and are certain that you need to disable it. Disabling this option would likely cause some list messages to be rejected by some receiving servers, and in some cases it could cause the recipient to be automatically removed from list membership 191. Alternatively, you could enable the *Refuse messages from domains with restrictive DMARC policies* 189 option instead, which causes incoming messages to the list to be refused when coming from a domain with a restrictive DMARC policy.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Prepend 'Subject:' header text with name of list
This setting causes MDaemon to enclose the name of the list in brackets (e.g. [ListName]) and add it to the beginning of the `Subject:` in all messages sent to the list. This is enabled by default.

Append 'Subject:' header text with thread number
This switch allows you to toggle whether thread numbers will be displayed in the `Subject:` header of list messages. They are appended to the end of the subject line in braces and used as a pseudo thread number. Sorting your Inbox by subject will align list mail in chronological order. This option is disabled by default.

3.4.2.4 Subscription



Subscribe/Unsubscribe

Allow subscription requests
This option controls whether or not the list will allow subscription requests, either through specially formatted email messages or through autoresponders. For more information, see: Subscribing to Mailing Lists 196.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Confirm subscription requests
When this box is checked, MDaemon will attempt to confirm subscription requests by generating a unique code and then sending it in a message to the address requesting to join the list. If the person then replies to that confirmation message, MDaemon will automatically add the member to the list. Confirmation messages are time-sensitive, meaning that the user must reply to the message within the number of minutes designated below.

Confirm autoresponder generated unsubscription requests
When this box is checked, MDaemon will attempt to confirm subscription requests that are generating automatically via the Autoresponder 529 option, "*Add sender to this mailing list*." As with the previous option, MDaemon will generate a unique code and then send it in a message to the address waiting to be added the list. If the person then replies to that confirmation message, MDaemon will automatically add the member to the list. These confirmation messages are also time-sensitive and therefore must replied to within the number of minutes designated below.

Unsubscribe

Allow unsubscription requests
This option controls whether or not the list will allow unsubscription requests, either through specially formatted email messages or through Autoresponders. For more information, see: Subscribing to Mailing Lists 196.

Confirm unsubscription requests
When this box is checked, MDaemon will attempt to confirm requests to remove a member from the list, by generating a unique code and then sending it in a message to the address requesting to unsubscribe from the list. If the person then replies to that confirmation message, MDaemon will automatically remove the member from the list. Confirmation messages are time-sensitive, meaning that the user must reply to the message within the number of minutes designated below.

Confirm autoresponder generated unsubscription requests
When this box is checked, MDaemon will attempt to confirm unsubscription requests that are generating automatically via the Autoresponder 529 option, "*Remove sender from this mailing list*." As with the *Confirm unsubscription requests* option above, MDaemon will generate a unique code and then send it in a message to the address waiting to be removed from the list. If the person then replies to that confirmation message, MDaemon will automatically remove the member. These confirmation messages are also time-sensitive and therefore must replied to within the number of minutes designated below.

Confirmations must be received within [XX] minutes
This is the number of minutes that the recipient of a subscription or unsubscription confirmation message has before the message will expire. If this time limit is exceeded before MDaemon receives a reply to the message, then the address will not be added or removed from the list. The address would then need to submit a new request to join or leave the list. The default setting of this option is 7200 minutes (i.e. five days).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

This is a global value—it applies to all of your mailing lists rather than to the specific list you are editing.

Notify subscribers/unsubscribers on the status of their requests
When this checkbox is enabled, MDaemon will send a completion notification message to the user that has been subscribed/unsubscribed to the Mailing List.

Membership Limit

Limit this list's membership to [xx] members (0=no limit)
With this feature you can place an upper limit on the number of people who are allowed to subscribe to the Mailing List. Enter a zero into this field if you do not wish to limit list subscriptions.

This limit only applies to addresses subscribed via the email methods outlined in *Subscribing to Mailing Lists* 196. This limit does not apply to subscriptions entered manually on the Members 186 screen, nor to subscription requests sent via email when the List password 202 is included.

See:

Subscribing to Mailing Lists 196
Autoresponder 529

3.4.2.4.1 Subscribing to Mailing Lists

Subscribing/Unsubscribing via Email Commands

To subscribe to or unsubscribe from a mailing list, send an email message addressed to `MDaemon` (or any alias thereof) at the domain hosting the mailing list, and place the `Subscribe` or `Unsubscribe` command as the first line of the message body. For example, there is a mailing list called `MD-Support` being hosted by `altn.com`. You can subscribe to the list by composing a message addressed to "`mdaemon@altn.com`" and placing the value: `SUBSCRIBE MD-Support@altn.com` as the first line of the message body. The message subject is irrelevant and can be left blank.

For complete details on how to form this and other control messages, see: Remote Server Control Via Email 678.

Occasionally, users will attempt to subscribe/unsubscribe to lists via email by sending the commands to the list itself rather than to the MDaemon system account. This results in the command being posted to the list rather than the user being subscribed or unsubscribed. To help prevent these sorts of

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

> messages from being posted to mailing lists, there is an option located at Setup » Preferences » System 347, called "*Screen incoming mailing list mail for obvious non-list content*." This option is enabled by default.

Subscribing/Unsubscribing via Email Addresses

The option, "*Honor '<List>-subscribe' and '<List>-unsubscribe' addresses*," located at Setup » Preferences » Miscellaneous 354, makes it possible for users to join or quit mailing lists by sending a message to a special email address rather than requiring them to use the email commands described in *Subscribing/Unsubscribing via Email Commands* above. To use this method to join or quit a list, a user would simply send a message to the list's address, but with "`-subscribe`" or "`-unsubscribe`" appended to the mailbox portion of the address. For example, if the list's name is, "franks`-list@example.com`," then a user could subscribe to the list by sending a message to, "`franks-list-subscribe@example.com`." To unsubscribe from the list, the message would be sent to, "`franks-list-unsubscribe@example.com`." In both cases the content of the subject and message body is irrelevant. Also, when this feature is active MDaemon will insert the following header into all list messages:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

Some mail clients can pick up on this and make an UNSUBSCRIBE button available to users automatically.

Subscribing/Unsubscribing via Autoresponders

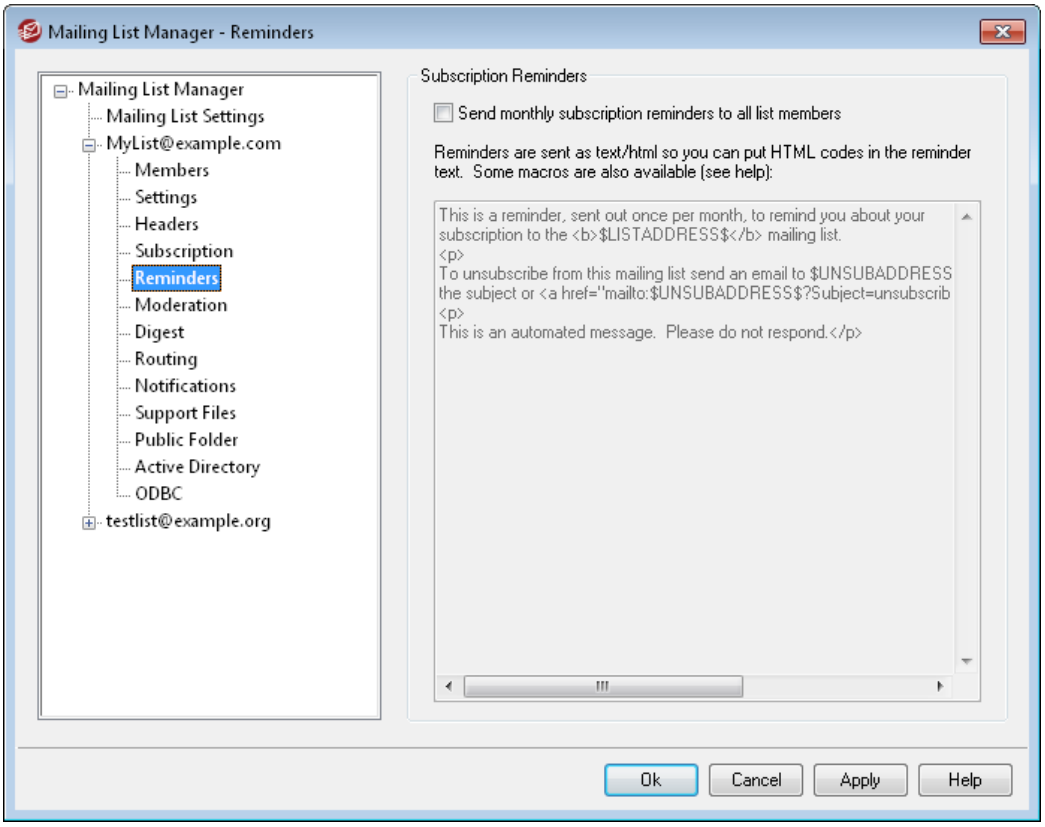
You can also utilize Autoresponders 529 to automatically add or remove list members. To do this you would create one or more MDaemon accounts whose sole purpose would typically be to automatically add or remove addresses who send messages to those accounts, via the Autoresponders configured for each account. For example, if you had a mailing list called, "`franks-list@example.com`," then you could create an MDaemon account with the address: "`join-franks-list@example.com`." You would then configure an autoresponder for that account to add to "`franks-list@example.com`" any addresses sending messages to it. Then, to join that list, all someone would have to do is send an email to "`join-franks-list@example.com`". This is a simple solution for users because it doesn't require them to remember any of the special email commands required by the *Subscribing/Unsubscribing via Email Commands* method outlined above.

See:

Subscription 194
Remote Server Control via Email 678
Autoresponder 529
Preferences » System 347
Preferences » Miscellaneous 354

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.4.2.5 Reminders



Subscription Reminders

Send monthly subscription reminders to all list members
Enable this option if you wish to send the contents of the provided text box as a subscription reminder message to each list member on the first day of each month. The reminder message is sent as text/html so that you can use HTML code in the reminder text if you choose. The following macros are available for use within the reminder message:

$LISTADDRESS$ - expands to the mailing list's email address (e.g. MyList@example.com)

$LISTNAME$ - expands to the local-part of the mailing list's email address (e.g. MyList).

$UNSUBADDRESS$ - expands the list's unsubscribe address (the MDaemon system address, e.g. mdaemon@example.com)

$MEMBERADDRESS$ - expands to the email address of the list member receiving the reminder (e.g. frank.thomas@example.com)

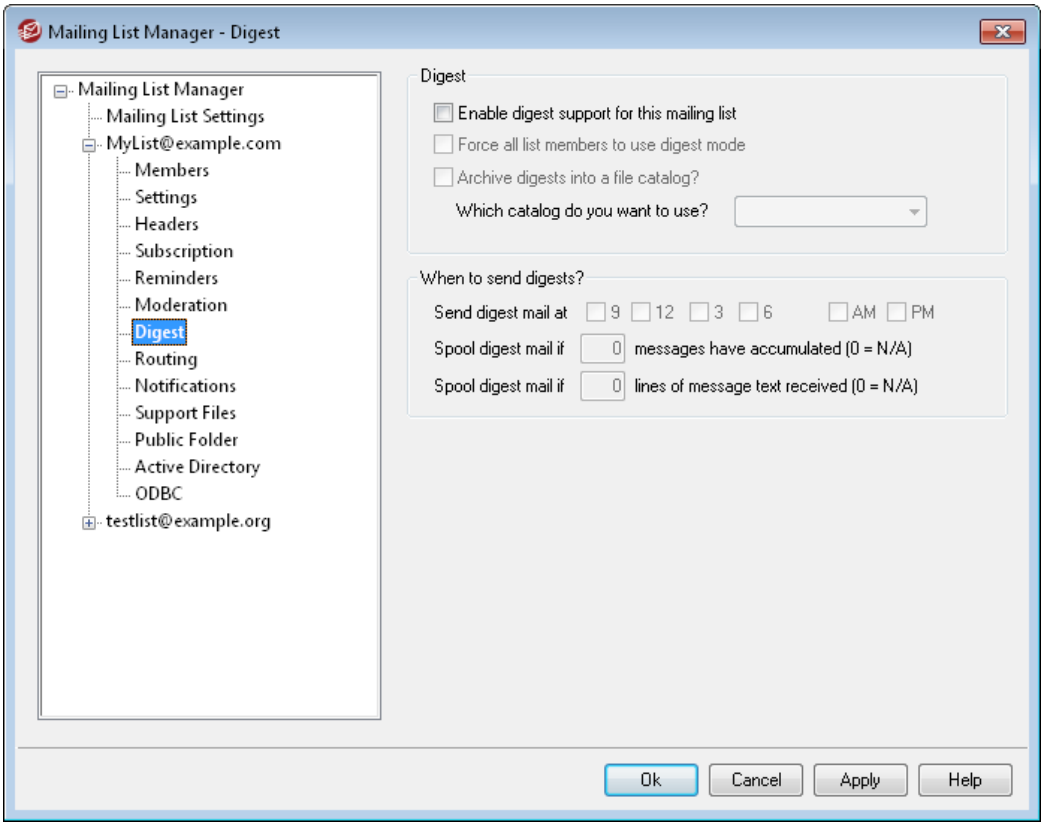
If you wish to send reminders on a different day of the month, you can do so by setting the following key in the MDaemon.ini file:

```
[Special]
ListReminderDay=X
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Set "X" to a number from 1 to 28, representing that day of the month you wish to send reminders.

3.4.2.6 Digest



Digest

Enable digest support for this mailing list
Check this box if you wish to allow digest support for this mailing list. When digest support is enabled, a copy of each message sent to the mailing list will be archived so that list members who have their membership type 186 set to *Digest* will periodically be sent batches of these archived messages in a compact and indexed format rather than receive them one at a time.

Force all list members to use digest mode
By default, list members can control whether they wish to receive list traffic in digest or normal format. Check this box if you wish to force all members to use digest mode, regardless of the mode they may have chosen for themselves.

Archive digests into a file catalog / which catalog do you want to use?
These options allow you to place digest messages into a file catalog so that back-issues of the digests can be collected in the future. MDaemon will generate a unique archive name for each digest and place it into the catalog you specify.

For complete information on how to work with catalogs see: Catalog Editor 650.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

When to send digests?

The following options determine how often and under what circumstances digests will be sent to those list members who are set to receive mail in digest format. All of the options operate independently of each other, meaning that any or all of them can cause a digest to be sent.

Send digest mail at 9, 12, 3, 6 AM and/or PM
Use this option to schedule how often this list's digests will be sent. If you check all of the boxes in this option then digests will be sent every three hours, in addition to any that may be triggered by the options below.

Spool digest mail if [xx] messages have accumulated (0 = n/a)
If you wish to send digests automatically whenever a certain number of messages have accumulated, specify that number here. Use "0" if you do not wish to use this option. "0" is the default setting.

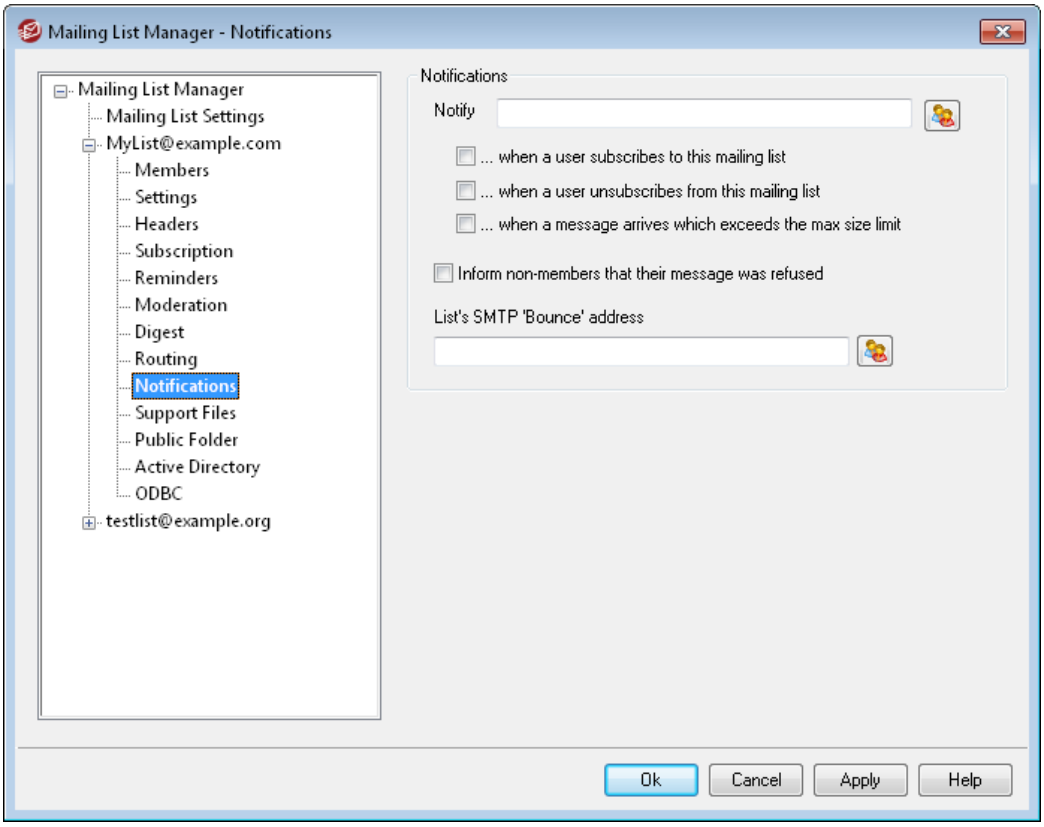
Spool digest mail if [xx] lines of message text received(0 = n/a)
Entering a value in this option will cause digests to be sent immediately whenever a digest grows to the number of lines of text specified. Use "0" if you do not wish to use this option. "0" is the default setting.

See:

Members 186
Catalog Editor 650
Remote Server Control via Email 678

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.4.2.7 Notifications



Notifications

Notify
Use this option to list an address that will be notified when the selected events take place.

...when a user subscribes to this mailing list
Check this box if you wish to send a note to the designated address each time someone subscribes to the mailing list.

...when a user unsubscribes from this mailing list
Check this box if you wish to send a note to the designated address each time someone unsubscribes from the mailing list.

...when a message arrives which exceeds the max size limit
Check this box if you wish to send a note to the designated address each time someone sends a message to the mailing list that is larger than *List refuses messages larger than [xx] KB* limit designated on Settings 189.

Inform non-members that their message was refused
When this option is enabled and non-members of a private list send mail to the list, MDaemon will inform them that the list is private. They will also be given instructions on how to subscribe to list. Lists are designated as private by using the *Only list*

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

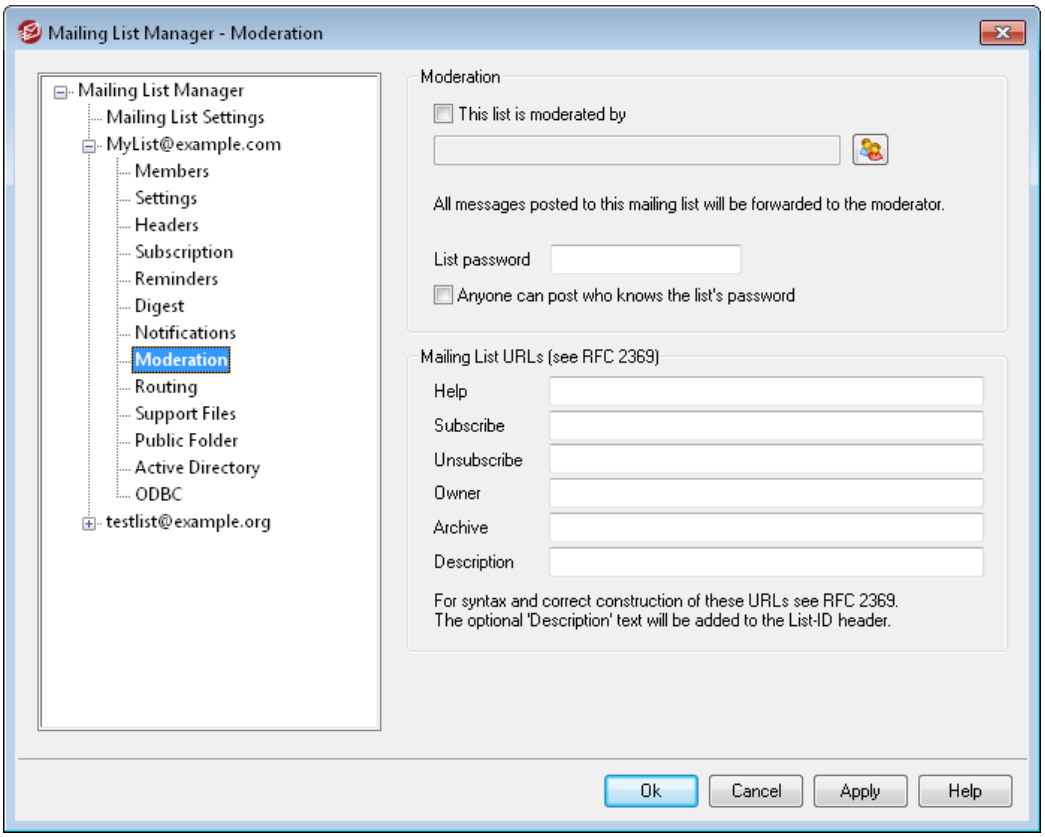
members can post to this list option located on Settings 189.

Returned Mail

List's SMTP 'Bounce' address
Use this option to specify the address that should receive any "bounced" mail or deliver status notification messages generated from list traffic. Any given message to a mailing list with 100 recipients might have, for example, ten undeliverable addresses due to address changes, down servers, or the like. The SMTP system will generate and return to the sender of the message a notification message concerning these undeliverable conditions. Using this option you can designate the address that should receive these messages for your mailing lists. You can also choose for no one to receive them, in which case MDaemon will place list mail into the mail stream in such a way that return mail will not be possible. This address should NOT be the mailing list's address.

Setting the *List's SMTP 'Bounce' address* to a local user's address could cause that user's email to be deleted as a result of the list pruner settings designated on Mailing List Settings 183. Use caution before setting this option to a local user's address. For more information, see Enhanced List Pruning 191.

3.4.2.8 Moderation



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Moderation

This list is moderated by
Check this box and specify an account if you wish the list to be moderated by the designated user. Moderated lists forward all posts to the moderator. The moderator alone may submit or forward messages to the list.

List password
If you wish to assign a password to this list, then enter it here. List passwords can be used with the *Anyone can post who knows the list's password* option below, and to override the *Membership Limit* option located on the Subscription screen 194. They also provide access to a number of features outlined in the *Remote Server Control via Email* 678 section.

Anyone can post who knows the list's password
If a password is assigned to the list, and this option is enabled, then anyone who includes the list's password at the beginning of a message's subject can post to the list, even if the list is moderated but the sender isn't the moderator.

Mailing List URLs (see RFC 2369)

MDaemon can add to mailing list messages any of the six header fields outlined in RFC 2369: *The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields*. The six headers are: **List-Help**, **List-Subscribe**, **List-Unsubscribe**, **List-Post**, **List-Owner**, and **List-Archive**. If you wish to use any of these headers to the list's messages, enter the desired header value into any of the fields below. The header values must be formatted according to the RFC 2369 specification (for example, `<mailto:list@example.com?subject=help>`). See the linked document for several examples of each header. MDaemon makes no changes to this data, therefore if the data is improperly formed it won't achieve any results.

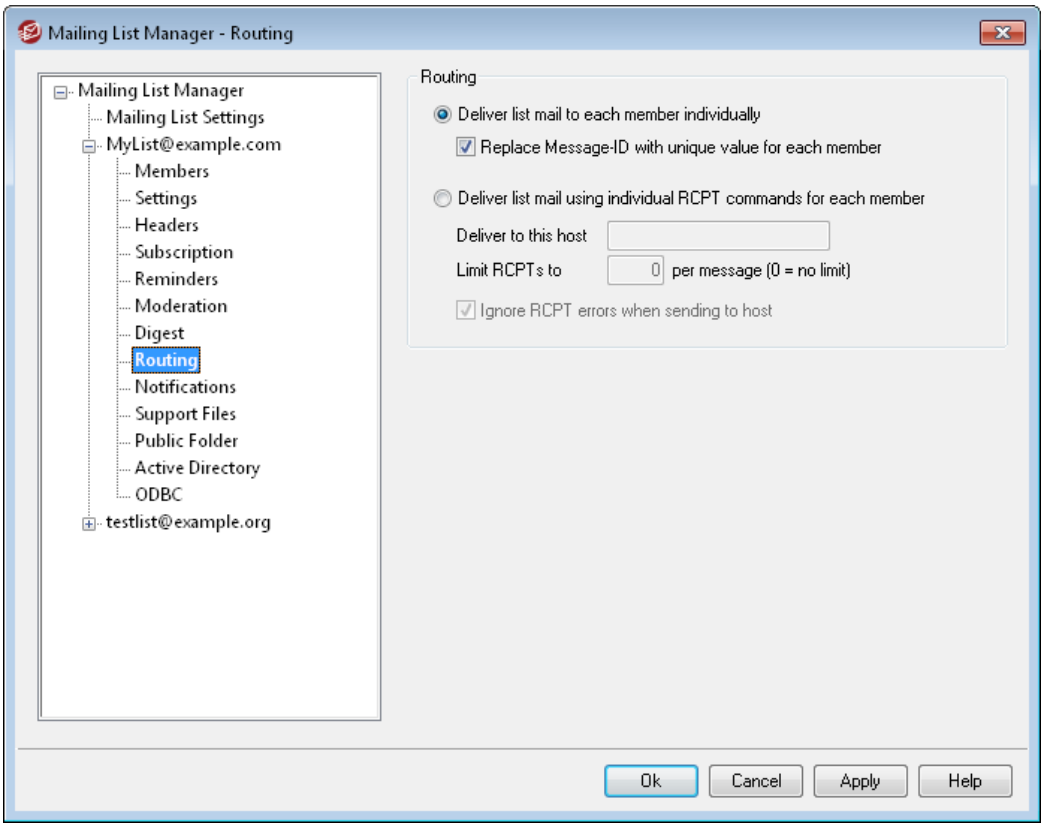
Description (used in List-ID: header)
Enter a short description of your mailing list here if you wish to add it to the `List-ID:` header included in messages that are sent to the list. The description and the list's identifier will be included in the header (e.g. `List-ID: "Frank's personal mailing list" <MyList.example.com>`) Note that the list's identifier is the mailing list's address with "." substituted for "@" in order to comply with the List-ID specification. If you leave the *Description* option blank then the List-ID: header will contain only the list identifier (e.g. `List-ID: <MyList.example.com>`). If an incoming message addressed to the list has a preexisting List-ID: header, MDaemon will replace the old header with the appropriate one for the list.

The List-Subscribe and List-Unsubscribe headers are included by default in all mailing list messages when the "*Honor '<List>-subscribe' and '<List>-unsubscribe' addresses*" option is enabled on the Preferences » Miscellaneous 354 screen. If you wish to override that option for this list, using different header values than those added automatically by that option, enter the desired values here. If that option is disabled then no List-

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Subscribe and List-Unsubscribe headers will be added to list messages unless you specify a value for them here.

3.4.2.9 Routing



Routing

Deliver list mail to each member individually
If selected, when messages are received for distribution to the list, a separate copy of each message will be created and dispatched to each list member. This will result in numerous individual messages being created which could affect the server's performance, depending on the size of the list and the load on the server.

Replace Message-ID with unique value for each member
When MDaemon is set to generate a separate copy of each message for each member, click this checkbox if wish each of those messages to have a unique Message-ID.

Deliver list mail using individual RCPT commands for each member
If selected, MDaemon will route a single copy of each list message to the specified smart host, rather then send individual messages to each member. This method employs multiple `RCPT To` statements during the SMTP session with the specified host.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

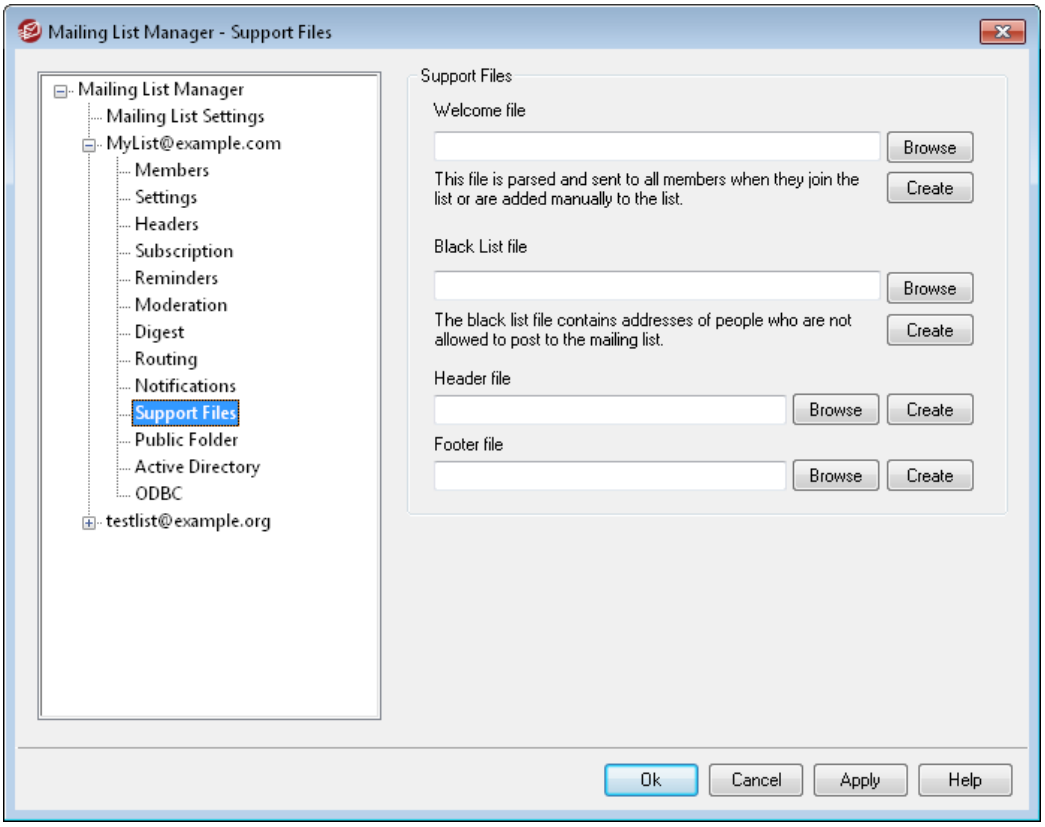
Deliver to this host
Designate the smart host to which you wish to pass all of the list's messages for delivery, using RCPT To statements for each member.

Limit RCPTs to [xx] per message (0=no limit)
Some hosts limit the number of `RCPT To` statements that they will accept when you are attempting to route a single copy of a message through them. If you specify the limit in this control then MDaemon will work around it by creating additional copies of the message and dividing the list into smaller groups. Then it will deliver the message to those groups thus avoiding the need to exceed the limitation. This is similar to the *Deliver list mail to each member individually* option above, but it generates less copies, sending each copy to groups of addresses rather than generating a separate copy for each member.

Ignore RCPT errors when sending to host
Since some smart hosts will refuse to queue or spool mail for certain domains, the routed approach to list delivery could cause numerous problems. An error code returned from the smart host as a result of this refusal would ordinarily cause MDaemon to abort the delivery attempt. Check this option if you want MDaemon to ignore error codes returned from the smart host during delivery of routed list mail, thus allowing those members that are accepted a chance to receive the message.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.4.2.10 Support Files



Support Files

Welcome File
If specified, the file listed here will be processed and have its contents emailed to all new members just after they subscribe. You may use the following macros in a new member welcome file:

`$PRIMARYDOMAIN$`	This macro expands to MDaemon's Default Domain name, which is designated on the Domain Manager.
`$PRIMARYIP$`	This macro will return the IPv4 address associated with MDaemon's Default Domain.
`$PRIMARYIP6$`	This macro will return the IPv6 address associated with MDaemon's Default Domain.
`$DOMAINIP$`	This macro will return the IPv4 address associated with the domain.
`$DOMAINIP6$`	This macro will return the IPv6 address associated with the domain.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

`$MACHINENAME$`	This macro returns the contents of the FQDN option designated on the Domain screen.
`$LISTEMAIL$`	Displays the list's email address. Example: `MyList@example.com`
`$LISTNAME$`	Displays the name of the mailing list. Example: `MyList`
`$LISTDOMAIN$`	This macro returns the mailing list's domain. Example: `example.com`
`%SETSUBJECT%`	Use this macro to designate an alternate subject for the Welcome message. The designated subject text can include other list macros such as `$LISTEMAIL$`. Example: `%SetSubject% =Welcome to the $LISTNAME$ list.`

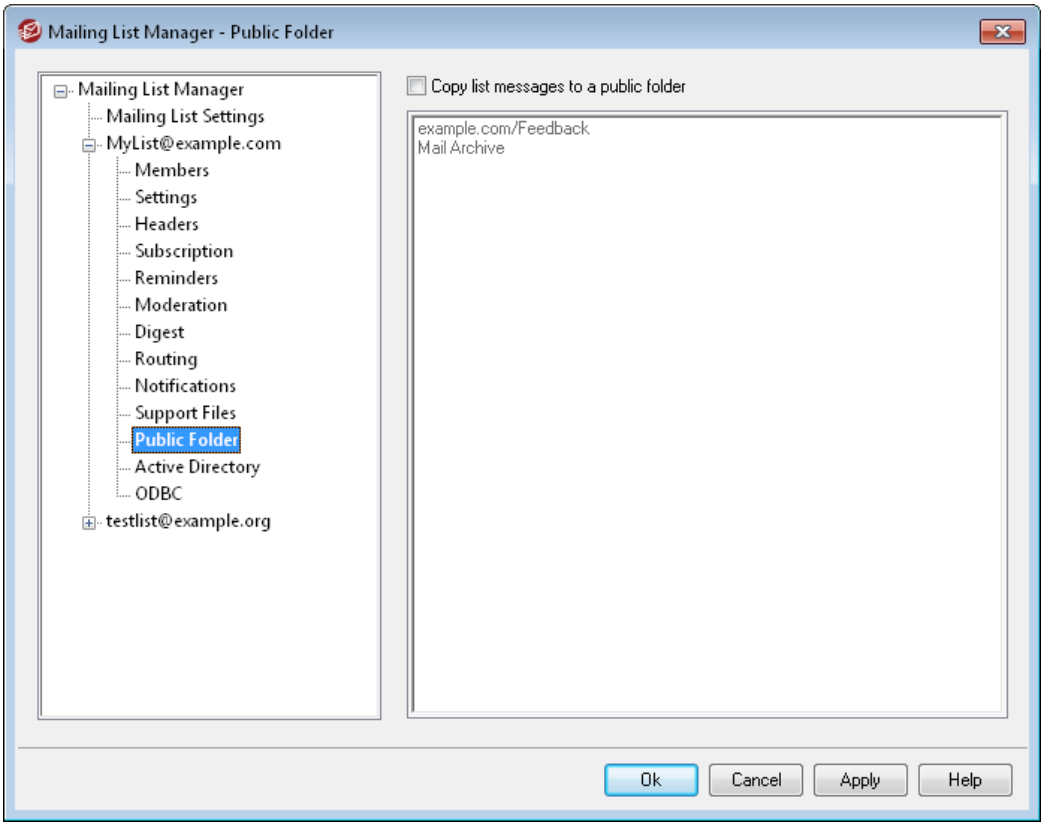
Black List File
If specified, the file listed here will be used to suppress messages sent from specified users.

Header/Footer File
The contents of the files specified here will be used as the header and/or footer file for list messages.

Create
To create a new file, click the *Create* button that corresponds to the file that you wish to create, specify a name, and then click *Open*. This will open the newly created file in Notepad for you to edit.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.4.2.11 Public Folder



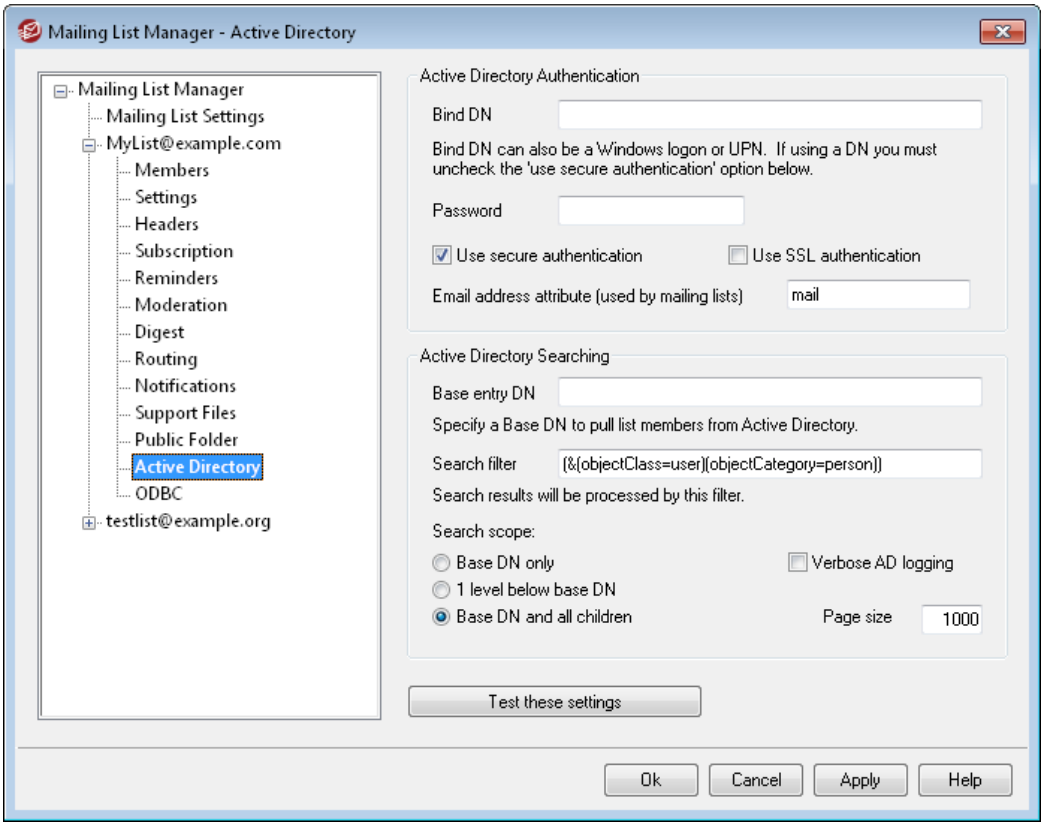
MDaemon supports using Public IMAP Folders 84 with mailing lists. Unlike personal IMAP folders, which are typically only accessible by a single user, Public folders are extra folders that are available to multiple IMAP users. The options on this screen are used to cause all messages destined for the Mailing List to be automatically copied to one of your public folders.

Copy list messages to a public folder
Enable this control if you want this list's messages to be copied to one of your Public Folders in addition to being delivered to the list.

Select a public folder
Click the Public Folder that you wish to associate with this list's messages.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.4.2.12 Active Directory



Use the options on this screen if you wish to pull some list member addresses from Active Directory.

Active Directory Authentication

Bind DN
This is the DN that MDaemon will use when binding to Active Directory using LDAP. Active Directory permits the use of a Windows account or UPN when binding.

When using a DN in this option rather than a Windows logon, you must disable/clear the "*Use secure authentication*" option below.

Password
This is the password that corresponds to the DN or Windows logon used in the *Bind DN* option above.

Use secure authentication
Click this checkbox if you wish to use secure authentication when performing your Active Directory searches. You cannot use this option when you are using a DN rather than a Windows logon in the *Bind DN* option above.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Use SSL authentication
Click this checkbox if you wish to use SSL authentication when performing your Active Directory searches.

Use of this option requires an SSL server and infrastructure on your Windows network and Active Directory. Contact your IT department if you are unsure if your network is setup this way, and to find out if you should enable this option.

Email address attribute
You must use this field to specify the attribute that will contain the email addresses used by this list. For example, if you used "`Mail`" in this field, then each Active Directory account that you wish to be treated as a list member must have the "`Mail`" attribute, and that attribute must contain an email address.

Active Directory Searching

Base entry DN
Specify the Distinguished Name (DN) or starting point in the Directory Information Tree (DIT) at which MDaemon will search Active Directory for addresses. You can use "`LDAP://rootDSE`" in this option to begin searching at Root DSE, which is the topmost entry in your Active Directory hierarchy. Designating a more precise starting point closer to the location of your user accounts or desired group of addresses in your particular Active Directory tree can reduce the amount of time required to search the DIT. Leave this field blank if you do not wish to pull any list addresses from Active Directory.

Search filter
This is the LDAP search filter that will be used when for searching Active Directory. Use this filter to enable MDaemon to more precisely locate the desired user accounts or addresses that you wish to treat as list members.

Search scope:

This is the scope or extent of your Active Directory searches.

Base DN only
Choose this option if you wish to limit your search to only the base DN specified above. The search will not proceed below that point in your tree (DIT).

1 level below base DN
Use this option if you wish extend your Active Directory search to one level below the supplied DN in your DIT.

Base DN and all children
This option will extend the scope of your search from the supplied DN to all of its children, down to the lowest child entry in your DIT.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

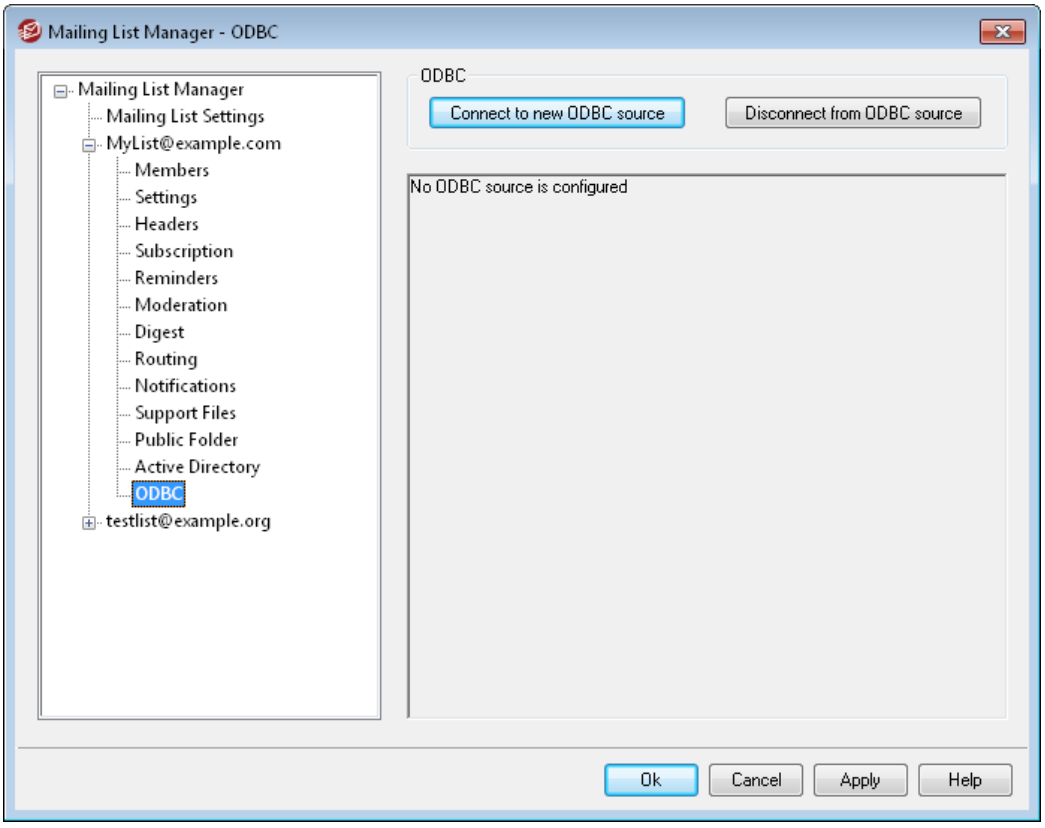
Page size
If the results of an Active Directory query exceed a specified number of entries, then they will be returned in separate "pages" in order to retrieve all the results. This setting is the maximum number of entries that will be included per page.

Verbose AD logging
By default MDaemon will use verbose logging for Active Directory. Clear this checkbox if you wish to use less extensive Active Directory logging.

Test these settings

Click this button to test your Active Directory configuration.

3.4.2.13 ODBC



Using this feature you can maintain the list's membership list in an ODBC compliant database. The ODBC screen of the Mailing List editor is used to select a data source, table, and field mappings for MDaemon to link to the list. When messages arrive for your list one or more SQL queries will be performed automatically and the resulting email addresses will be treated as part of the list's membership.

You can add, remove, and modify members of your list in the database using whatever ODBC compliant database application you choose.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

ODBC

This section displays the current ODBC properties that you have set up for the mailing list. It displays the database's field mappings and the SQL queries that you have configured to designate each member's membership status (i.e. Normal, Post Only, Read Only, and/or Digest mode).

Connect to new ODBC source
Click this button to open the ODBC Selector Wizard for choosing the system data source that you wish to use for the mailing list.

Disconnect from ODBC source
Click this button to disconnect the list from the ODBC data source listed in the space above.

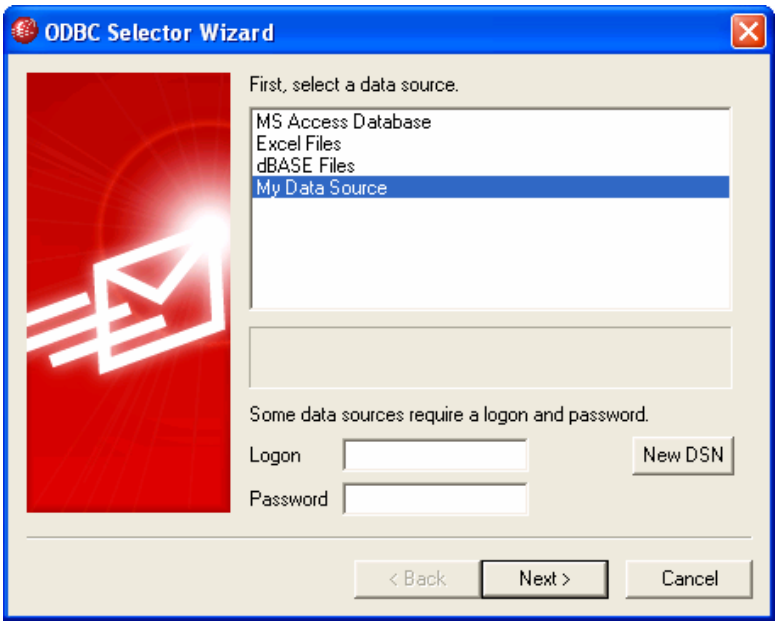
See:

Configuring an ODBC System Data Source for a Mailing List 212
Creating a New System Data Source 214

3.4.2.13.1 Configuring an ODBC Data Source

To use an ODBC accessible database with a mailing list:

1. On the ODBC screen 211 of the Mailing List editor, click **Connect to new ODBC source** to open the ODBC Selector Wizard.



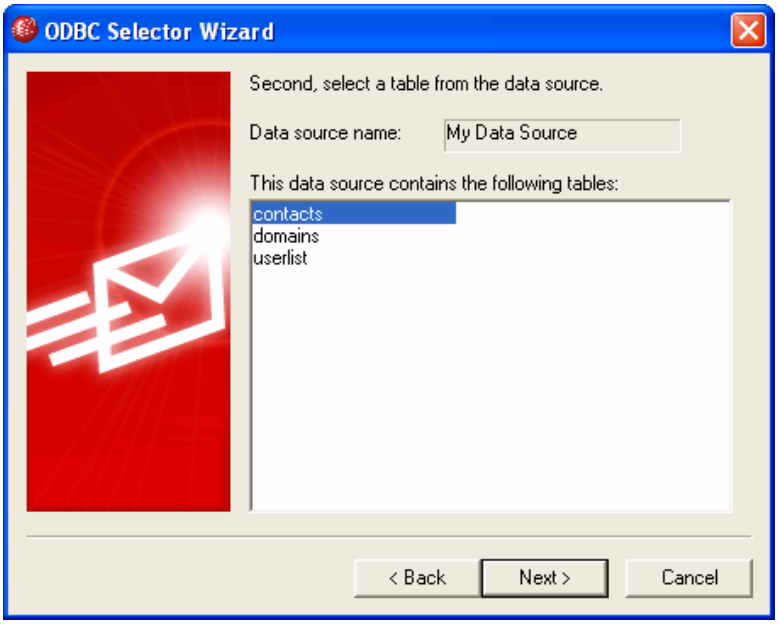
2. Select the **data source** that you wish to use for the list. If there is not a compatible data source listed, click **New DSN** and then follow the instructions listed under, **Creating a New ODBC Data Source** 214.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

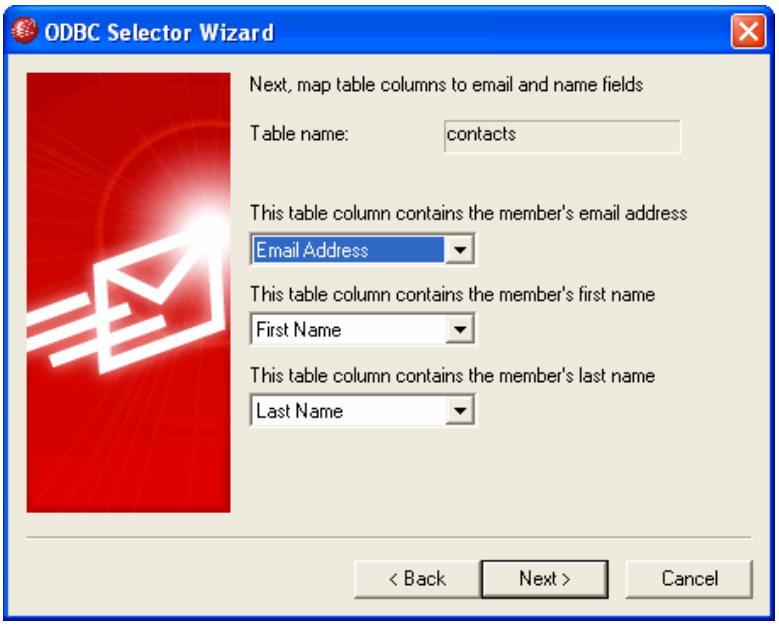
3. If required, enter the data source's **Logon** and **Password**.

4. Click **Next**.

5. The data source must contain at least one table with fields for email addresses and names. If the data source contains one or more qualifying tables, choose the desired table and click **Next**. Otherwise, click **Cancel** to exit the ODBC Selector Wizard and then use your database application to add a table to the relevant database before continuing.

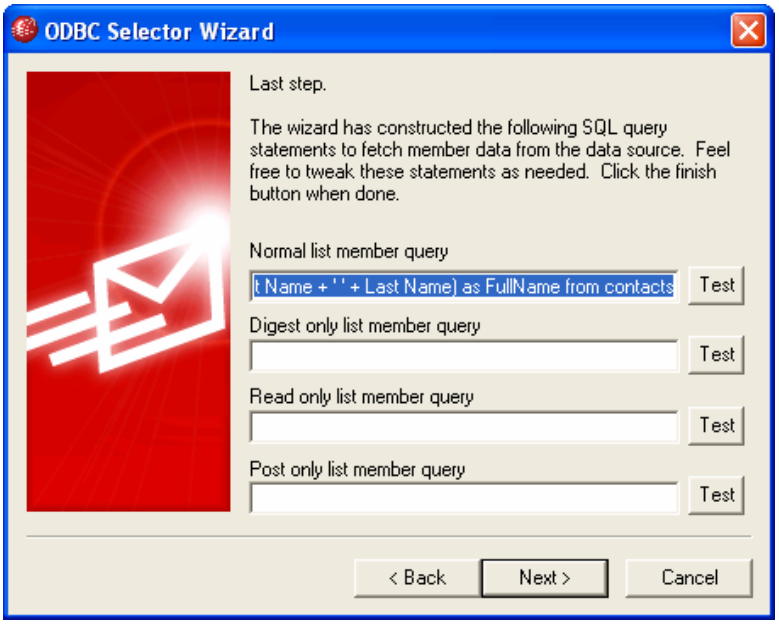


6. Use the drop-down list boxes to designate the table fields that will correspond to **email address**, **first name**, and **last name**. Click **Next**.


ODBC Selector Wizard
Next, map table columns to email and name fields
Table name:
contacts
This table column contains the member's email address
Email Address
This table column contains the member's first name
First Name
This table column contains the member's last name
Last Name
< Back
Next >
Cancel

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

7. The ODBC Selector Wizard will construct an SQL query statement based on your selections in **Step 6**. MDaemon will use it to retrieve normal list member data from your database. You can edit this statement as desired, and include other query statements in the remaining controls to cause members to receive messages in Digest mode, and to designate members as Read Only or Post Only. A **Test** button is provided beside each control so that you can test your query statements to make sure they retrieve the proper data. When you are finished configuring your query statements, click **Next**.


ODBC Selector Wizard
Last step.
The wizard has constructed the following SQL query statements to fetch member data from the data source. Feel free to tweak these statements as needed. Click the finish button when done.
Normal list member query
t Name + ' ' + Last Name) as FullName from contacts
Test
Digest only list member query
Test
Read only list member query
Test
Post only list member query
Test
< Back
Next >
Cancel

8. Click **Finish**.

See:

Mailing List Editor » ODBC 211
Creating a New ODBC Data Source 214

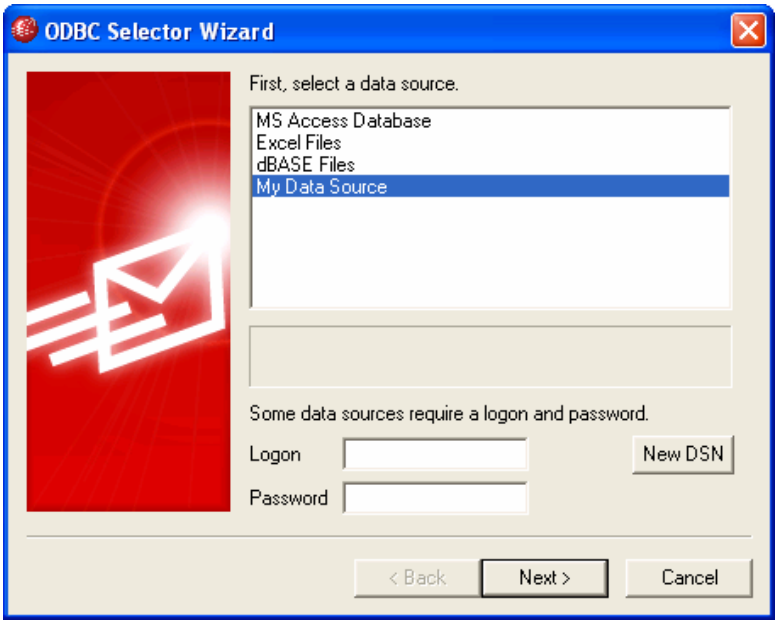
3.4.2.13.2 Creating a New ODBC Data Source

To create a new ODBC system data source for use by a mailing list:

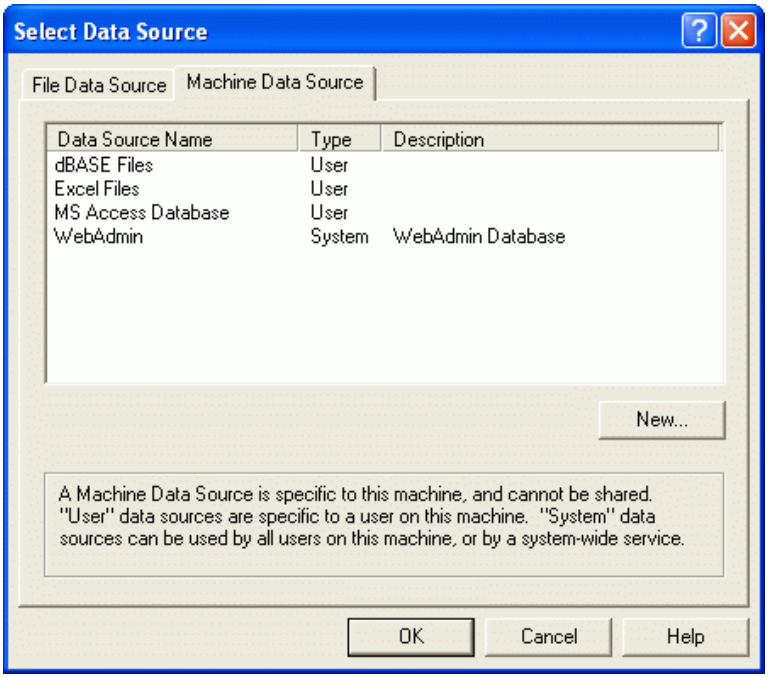
1. On the ODBC screen 211 of the Mailing List editor, click **Connect to new ODBC source** to open the ODBC Selector Wizard.

2. Click **New DSN** to open the Select Data Source dialog.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

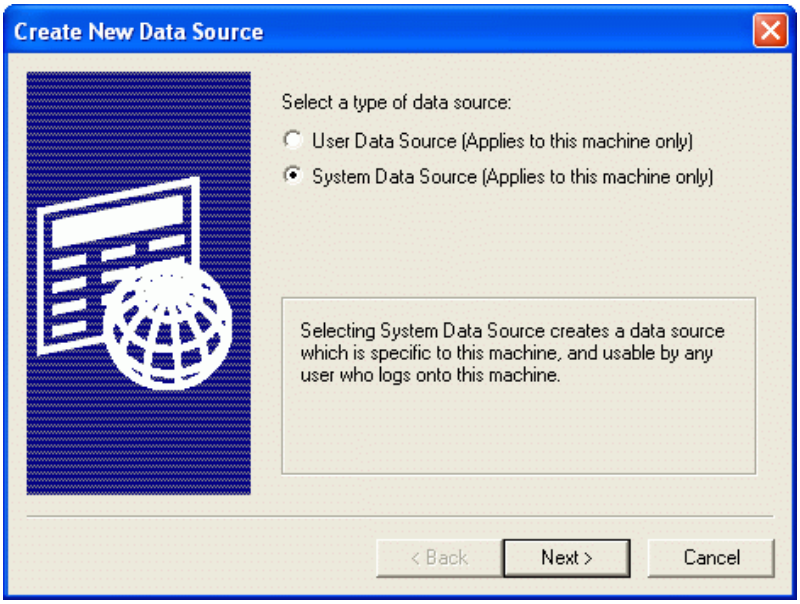


3. Switch to the **Machine Data Source** tab, and click **New...** to open the Create New Data Source dialog.

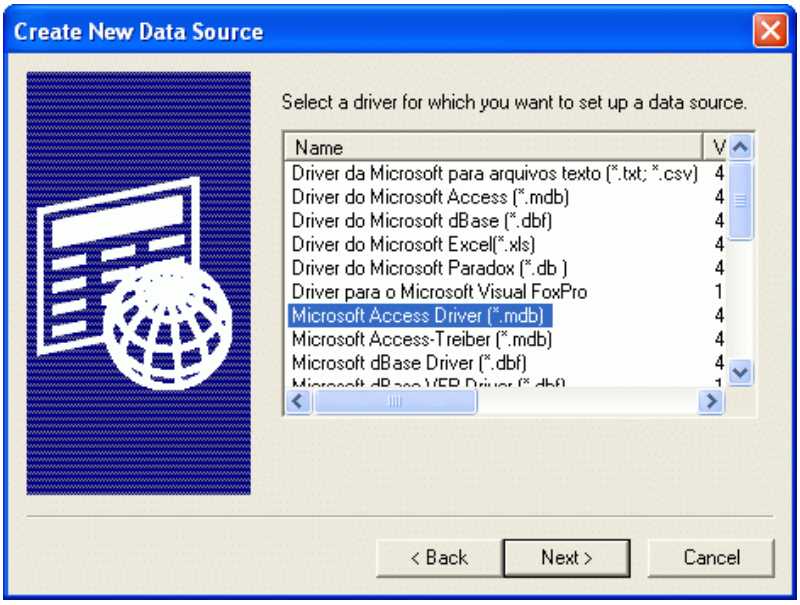


4. Select **System Data Source**, and click **Next**.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

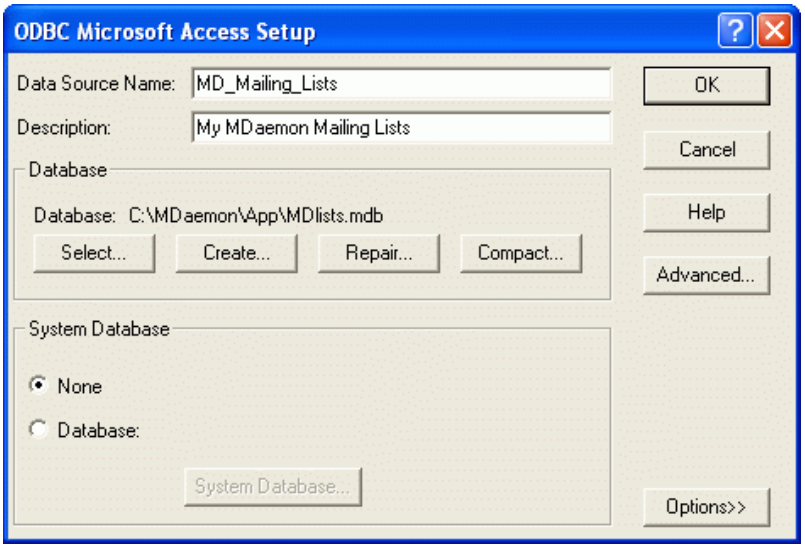

Create New Data Source
Select a type of data source:
User Data Source (Applies to this machine only)
System Data Source (Applies to this machine only)
Selecting System Data Source creates a data source which is specific to this machine, and usable by any user who logs onto this machine.
< Back
Next >
Cancel

5. Select the **database driver** for which you wish to set up the data source, and click **Next**.


Create New Data Source
Select a driver for which you want to set up a data source.
Name
Driver da Microsoft para arquivos texto (*.txt; *.csv)
Driver do Microsoft Access (*.mdb)
Driver do Microsoft dBase (*.dbf)
Driver do Microsoft Excel(*.xls)
Driver do Microsoft Paradox (*.db)
Driver para o Microsoft Visual FoxPro
Microsoft Access Driver (*.mdb)
Microsoft Access-Treiber (*.mdb)
Microsoft dBase Driver (*.dbf)
< Back
Next >
Cancel

6. Click **Finish** to display the driver-specific setup dialog. The appearance of this dialog will vary based on which driver you have selected (Microsoft Access Setup dialog shown below).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



7. Designate a **Data Source Name** for your new data source and provide any other information required by the driver-specific dialog (such as creating or specifying a database, choosing a directory or server, and so on).

8. Click **OK** to close the driver-specific dialog.

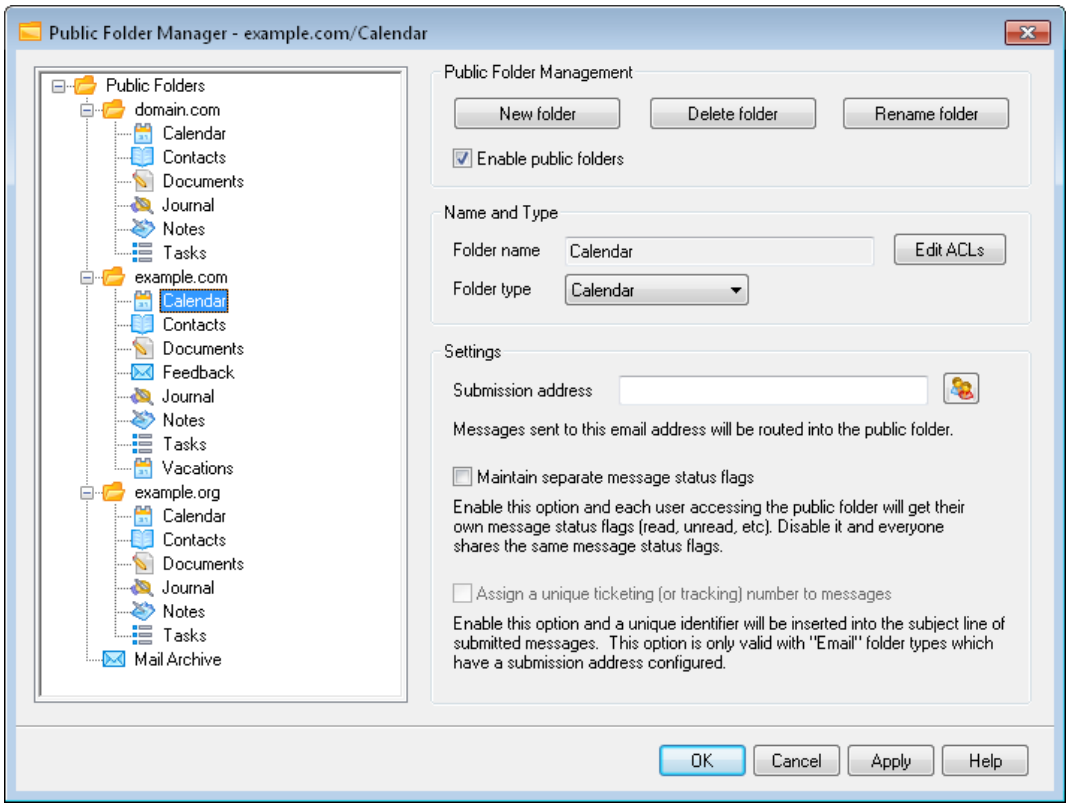
9. Click **OK** to close the Select Data Source dialog.

See:

ODBC - Mailing Lists 211
Configuring an ODBC System Data Source for a Mailing List 212

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.5 Public Folder Manager

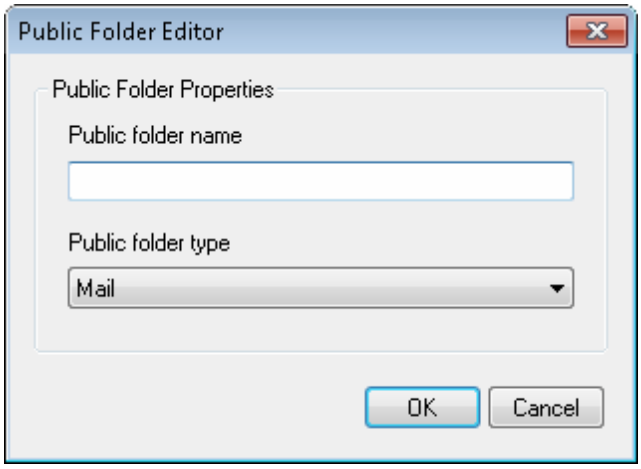


Use this screen to manager your public folders[84]. To reach the Public Folder Manager, click "Setup » Public Folder Manager...".

Public Folder Management

New folder

To create a new public folder, select the folder in the list that you wish to be its parent folder, and click *New folder*. Enter a name for your folder, choose the folder type, and click *OK*.



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Delete folder
To remove a public folder from the list, select the desired folder and then click the *Delete folder* button.

Rename folder
To rename a public folder, select a folder and click *Rename folder*. Type a new name and click *Ok*.

Enable public folders
Click this check box if you wish to allow users to gain access to public folders. The users that can access them and the level of access granted is controlled by selecting a folder and clicking the *Edit ACLs* button.

Name and Type

Folder name
This box displays the name of the folder you have selected in the list. The remaining options on this screen apply to the selected folder.

Folder type
Use the drop-down list to designate the type of folder: Mail, Contacts, Calendar, etc.

Edit ACLs
Choose a folder and then click this button to open the Access Control List 220 dialog for that folder. Use the Access Control List to designate the users or groups that will be able to access the folder and the permissions for each user or group.

Settings

Submission address
Use this option to associate a specific account with a shared folder so that messages destined for that *Submission Address* will be automatically routed to the shared folder. However, only users who have been granted "post" permission to the folder will be able to send to that address.

Maintain separate message status flags
Click this check box if you want the folder's message flags (read, unread, replied to, forwarded, and so on) to be set on a per-user basis instead of globally. Each user will see the status of the messages in the shared folder displayed according to his or her personal interaction with them. A user who hasn't read a message will see it flagged as 'unread' while a user who has read it will see the status as 'read'. If this option is disabled then all users will see the same status. So, once any user has read a message then all users will see it marked as 'read'.

Assign a unique ticketing (or tracking) number to messages
Use this option if you wish to configure the public folder as a message ticketing public folder. MDaemon will add the *Folder name* and a unique identifier to the subject of messages sent to the public folder's *Submission address*. Any outbound messages having this specially formatted subject will have the From address changed to the submission address of the public folder and a copy of the outbound

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

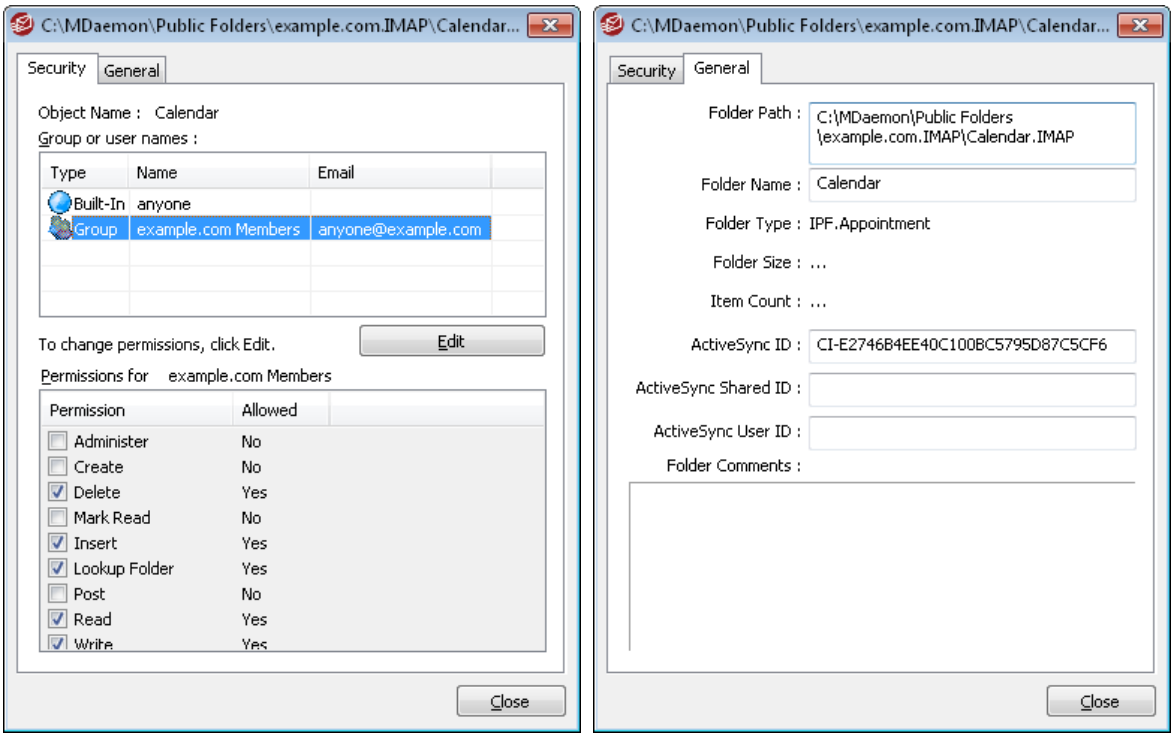
message will be placed into a child public folder named "Replied To". In addition, any inbound messages with this specially formatted subject will be automatically redirected to the public folder, regardless of the address the message was sent to.

See:

Access Control List 220
Public Folders Overview 84
Public & Shared Folders 87
Account Editor » Shared Folders 547
Mailing List » Public Folders 208

3.5.1 Access Control List

The Access Control List (ACL) is used for setting user or group access permissions for your public and shared folders 84. It is accessed from the *Edit ACLs* button on the Public Folder Manager 218 or the *Edit access control list* button on Account Editor's Shared Folders 547 screen.



Security

This tab displays the list of groups or users associated with the folder and the specific access permissions granted to each. Select a group or user in the list to display its permissions 221 for review in the Permissions window below. To edit the permissions, click **Edit** 221.

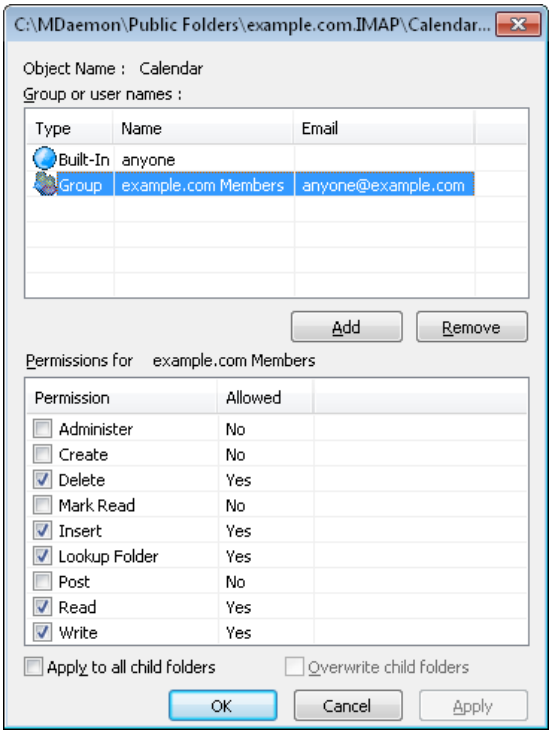
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

General

This tab displays the folder's properties, such as its path, name, type, size, and so on.

ACL Editor

Click **Edit** on the ACL's Security tab to open the ACL Editor for modifying access permissions.



Object Name
This is the name of the object or folder to which the ACL permissions will apply.

Group or user names
These are the groups or users to which some level of access permissions may have been granted. Select a group or user to display its permissions in the *Permissions for <group or user>* window below. Check the box next to any access permission that you wish to grant to the group or user.

Add
To grant access permissions to a group or user not listed above, click **Add** 222.

Remove
To remove a group or user, select its entry in the list above and click **Remove**.

Permissions for <group or user>
Check the box next to any access permission that you wish to grant to the group or user selected above.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

You can grant the following access control permissions:

Administer – user can administer the ACL for this folder.

Create – user can create sub-folders within this folder.

Delete – user can delete items from this folder.

Mark Read – user can change the read/unread status of messages in this folder.

Insert – user can append and copy items into this folder.

Lookup Folder – user can see this folder in his personal list of IMAP folders.

Post – user can send mail directly to this folder (if folder allows).

Read – user can open this folder and view its contents.

Write – user can change flags on messages in this folder.

Apply to all child folders
Check this box if you wish to apply this folder's access control permissions to any sub-folders it currently contains. This will add the folder's user and group permissions to the child folders, replacing them when there are any conflicts. It will not, however, delete any other user or group permissions that currently have access to those folders.

Example,

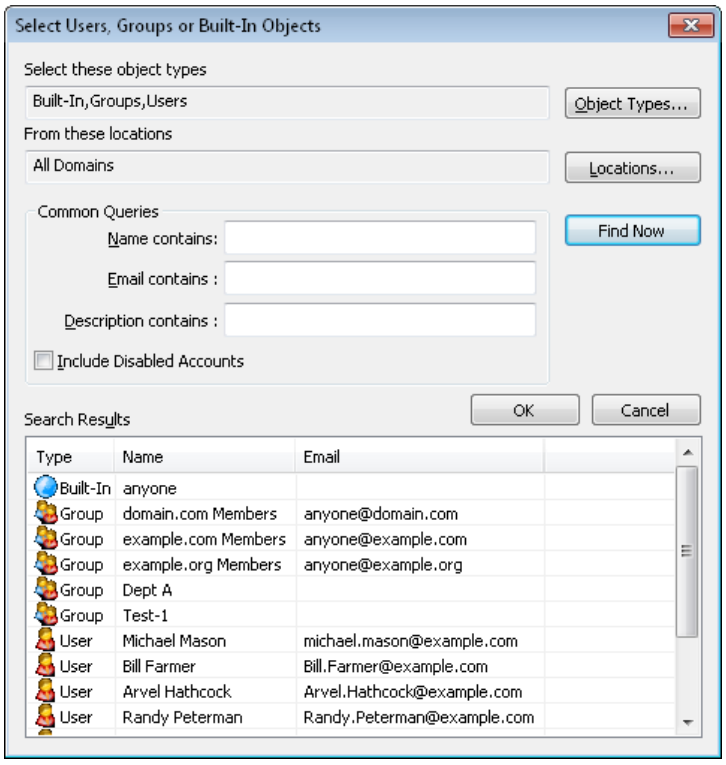
The parent folder grants certain permissions to `User_A` and `User_B`. The child folder grants permissions to `User_B` and `User_C`. This option will add `User_A` permissions to the child folder, replace the child folder's `User_B` permissions with those from the parent folder, and do nothing to the `User_C` permissions. Therefore the child folder will then have `User_A`, `User_B`, and `User_C` permissions.

Overwrite child folders
Check this box if you wish to replace all child folder access permissions with the parent folder's current permissions. The child folder permissions will then be identical to the parent folder.

Adding a Group or User

Click **Add** on the ACL Editor if you wish to add another group or user to the Access Control List. This opens the Add Group or User screen that you can use to search for them and then add them.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Select these object types
Click **Object Types...** to select the object types that you wish to search for the groups or users you wish to add. You can select: Built-In, Groups, and Users.

From these locations
Click **Locations...** to select the domains that you wish to search. You can select all of your MDaemon domains or specific domains.

Common Queries
Use the options in this section to narrow your search by specifying all or part of the user's name, email address, or the contents of the account's Description 521. Leave these fields blank if you want the search results to contain every group and user that matches the Object Types and Locations specified above.

Include Disabled Accounts
Check this box if you wish to include disabled accounts 521 in your search.

Find Now
After you have specified all of your search criteria, click **Find Now** to perform the search.

Search Results
After performing the search, select any desired groups or users in the Search Results and click **OK** to add them to the ACL. To select more than one group or user, hold down the Ctrl key when selecting them.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Access rights are controlled through MDaemon's support for Access Control Lists (ACL). ACL is an extension to the Internet Message Access Protocol (IMAP4), which makes it possible for you to create an access list for each of your IMAP message folders, thus granting folder access rights to other users who also have accounts on your mail server. If your email client doesn't support ACL you can still set the permissions via the controls on this dialog.

ACL is fully discussed in RFC 2086, which can be viewed at: http://www.rfc-editor.org/rfc/rfc2086.txt.

See:

Public Folder Manager 218
Public Folders Overview 84
Public & Shared Folders 87
Account Editor » Shared Folders 547
Mailing List » Public Folders 208

3.6 Web & IM Services

3.6.1 WorldClient (web mail)

3.6.1.1 Overview

WorldClient is a web-based email solution included in MDaemon and designed to offer users email client functionality using their favorite web browser. WorldClient can easily hold its own against traditional mail clients while providing the added bonus of its ability to enable users to access their email from anywhere at anytime as long as they have an Internet or network connection. Further, because all of their email folders, contacts, calendars, and so on reside on the server instead of on their local computer, they can have access to everything as if they were at their desk.

WorldClient provides many benefits to email administrators. Since WorldClient isn't workstation dependent you can configure everything from the server, unlike many client applications. This saves you from having to configure and maintain each individual email client. You can also customize the graphical images and HTML pages used in WorldClient to suit your corporate needs, or the needs of your customer. Further, you can give your users the ability to maintain their own account settings thus saving you time — you can give as much or as little control to your users as you want.

Finally, in addition to the convenience of having a web-based client, there are many additional features that will benefit your users, such as: extensive email functionality, client-side interface available in almost 30 languages, personal and global address books, manageable mail folders and filters, send/receive file attachments, multiple visual "themes" for the interface, themes for mobile devices, calendar features, groupware features, an integrated instant messenger that can be downloaded to your desktop, and much more.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Calendar & Scheduling System

MDaemon is equipped with a complete collaboration system. From within WorldClient you can easily create appointments, schedule meetings, and work with address books. Recurring appointments are fully supported, and appointments have many fields available to describe them. Further, contacts, calendars, and task data are stored as IMAP folders within each user's root mail directory. Through WorldClient, your users can access these personal folders and control which other users have access to them. All WorldClient themes (especially Lookout) have templates that present contact, calendar, notes, and task folders in a logical and attractive way.

Because the Calendar system is integrated with MDaemon, there is the added benefit of email notifications of appointments, whether scheduled by you or a third-party. Whenever someone other than yourself schedules an appointment for you, you will receive an email message summarizing the appointment. Each designated appointment attendee will receive an email message detailing the appointment's date, time, location, subject, and list of attendees. Further, any attendees who have calendar entries that conflict with the appointment's time slot will receive a message notifying them of the appointment and its conflict with their schedule. The person who scheduled the meeting will receive a summary message listing all of the meeting's details and invited attendees who did or did not have scheduling conflicts.

The Calendar System is also equipped with support for Internet Calendar (iCal) used by Microsoft Outlook and other iCalendar compliant email programs. The Calendar System can detect and process iCalendar information sent to your users and update their calendars accordingly. When a user opens an iCalendar attachment from within WorldClient the information contained in the attachment will be reflected in the user's WorldClient calendar. Also, when users create new meetings or appointments they can list one or more email addresses to which they wish an iCalendar email to be sent. This feature can be set by individual users in their WorldClient options.

WorldClient Instant Messenger

WorldClient Instant Messenger (WCIM) is MDaemon's secure instant messaging system, address book client, and tray applet that provides quick access to WorldClient's email features. WCIM can be downloaded by each WorldClient user and then installed on the individual's local computer. It is pre-configured for the specific user when downloaded, thus limiting the need to configure it manually.

WCIM runs in the background and checks your account for new mail by querying the WorldClient server directly. This eliminates the need to open a browser or keep one open to check your email — WCIM checks for new mail and notifies you with a sound or visual alert when new mail arrives. WCIM also displays a list of your mail folders and the number and type of messages that each one contains (new, unread, and read). Furthermore, it can be used to launch your browser and move it immediately to a specific mail folder, the first unread message, the compose page, or your calendar page.

Additionally, WCIM can be used to provide two-way address book synchronization between MDaemon and the Outlook/Outlook Express address book on each user's local computer. Thus, if you use both Outlook or Outlook Express and WorldClient at different times, the address books will match in both products.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Finally, WCIM is also equipped with a complete instant messaging system. You can view your list of WCIM "buddies" and each one's online status (online, away, offline), start a conversation with any one or group of them, set your own online status, and view past conversations in a history folder.

For specific instructions on how to use WorldClient Instant Messenger, see its online help system.

WorldClient Instant Messenger's Instant Messaging System

WCIM is equipped with a simple but effective instant messaging (IM) system. With this system you can communicate instantly with any other account on your MDaemon server. You can choose a list of "buddies" from a list of all MDaemon users and then see which ones are online and ready to receive an IM. You will also be able to start a group conversation involving several buddies at once. All of the IM features are available via the tray icon's shortcut menu, and from the WCIM window.

WorldClient Instant Messenger's IM system is also scriptable, which allows custom programs to interface with it. By creating semaphore (SEM) files in the \MDaemon \WorldClient\ folder, an external application can send instant messages to your WCIM users. The following is the format of the SEM file:

`To: user1@example.com`	Email address of WCIM user.
`From: user2@example.com`	Email address of instant message's sender.
`<blank line>`	
`Text of instant message.`	This is the text sent as an instant message.

The SEM file name must start with the characters "IM-" and be followed by a unique numerical value. For example, "IM-0001.SEM". Applications should also create a corresponding file called "IM-0001.LCK" to lock the SEM file. Once the SEM file is completed remove the LCK file and the SEM file will be processed. MDaemon uses this scripting method to send Instant Message reminders to you about upcoming appointments and meetings.

The Content Filter system is equipped with an Action that uses this scripting method to send instant messages. Further, rules utilizing this action can use the Content Filter macros in the IM. For example, you could create a rule to send an instant message rule containing lines like this:

```
You have received an email from $SENDER$.
Subject: $SUBJECT$
```

This rule would be an effective way to send new mail alerts through WCIM.

Because many businesses and administrators have reservations about using an Instant Messaging system in their company due to the inherent lack of centralized accountability and the inability to monitor IM traffic that is in traditional and well known IM clients, we have designed WCIM's instant messaging system to minimize those deficiencies. First of all, our system is not peer-to-peer — individual WCIM clients do not connect directly to each other. Further, because every IM passes through the server, each message is logged in a central location accessible to the MDaemon/

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

WorldClient administrator. Thus a record of all conversations can be maintained for the security of both your company and your employees or users. IM activity is logged in a file called `InstantMessaging.log` located in the `MDaemon\LOGS\` directory. The assurance of accountability is also the primary reason we do not support other IM clients such as ICQ, AOL, and MSN. Finally, WorldClient Instant Messenger's IM system is secure in that each transaction is strongly encrypted from start to finish so that plain text is never transmitted.

Instant Messaging is provided on a per-domain basis. Controls for activating instant messaging and designating whether or not IM traffic should be logged are located on the WorldClient Instant Messenger screen 239 of the WorldClient dialog (Setup » Web & IM Services » WorldClient (web mail) » WCIM).

WorldClient Instant Messenger Skins

WCIM's interface is compatible with *msstyles* skins, which are readily available on the internet. Several styles are included, but to install a new style, download the `*.msstyles` file and place it under WCIM's `\Styles\` folder in a subfolder with the same name as the file. For example, if the file was called `Red.msstyles` then the path for the file would be: "`\.\Styles\Red\Red.msstyles`"

Automatic Address Book Synchronization

By using WCIM in conjunction with MDaemon's integrated address book system, you can provide two-way synchronization between MDaemon and the Outlook/Outlook Express address book on each user's local computer. Thus, if you use both Outlook or Outlook Express and WorldClient at different times, the address books will match in both products.

MDaemon maintains an accurate and continuously up to date database of users each time an MDaemon account is added, removed, or modified. WCIM has the ability to query MDaemon at regular intervals and acquire all the contact information being stored there. It then publishes this information to the local computer's Windows Address Book or contact store. This has the effect of instantaneously updating any local software package which uses the local address book system (for example, Outlook/Outlook Express).

Anyone using WCIM with the proper access credentials can also add Public contacts by using the Windows Address Book directly, or through Outlook/Outlook Express. The new contact will be picked up by WCIM and uploaded to MDaemon's address book. From there all other users on your network will have access to the new contact the next time their WCIM queries MDaemon.

On the Synchronization screen of WCIM's Preferences dialog you can specify the folders within your Windows Address Book that you wish to be synchronized. You can designate separate folders for both Public and Private contacts.

Windows Address Book (WAB) synchronization requires IE 5 or greater with identity support enabled.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

End-to-end Email and Attachment Encryption

The WorldClient theme is equipped with support for end-to-end email and attachment encryption through Virtru. To enable this feature, the WorldClient user must switch to the WorldClient theme, go the the Options » Compose page, and click **Enable Virtru**. This causes a button to appear on the Compose page that the user can click to encrypt his or her email before sending. This is an easy-to-use feature that doesn't require the user to remember or save any special passwords or keys. Recipients who use a Virtru-enabled client such as the WorldClient theme, or one of Virtru's other client plugins, can open and read the encrypted messages normally, without any additional steps. Recipients without a Virtru-enabled client will see a link to view the message in a special browser-based reader.

If you wish to prevent your users from being able to use Virtru encryption within WorldClient, open the `Domains.ini` file in the `MDaemon/WorldClient` folder and add: `VirtruDisabled=Yes`.

For more information, see: Email Encryption.

Using WorldClient

Starting WorldClient

There are three ways to start/stop the WorldClient server:

1. In the Stats pane on the left-hand side of the MDaemon GUI, right-click on the WorldClient entry and choose the *Toggle Active/Inactive* selection on the shortcut menu.
2. Click "File » Enable WorldClient" server on the main interface.
3. Click "Setup » Web & IM Services" on the main interface, and then click *WorldClient runs using built-in web server* on the Web Server screen.

Logging in to WorldClient

1. Point your web-browser to `http://example.com:WCPortNumber`. This port is designated on the Web Server 229 screen of the WorldClient section. If you configure WorldClient to listen to the default web port (port 80) then you do not need to denote the port number in the login URL (e.g. `www.example.com` instead of `www.example.com:3000`).
2. Type your MDaemon account's user name and password.
3. Click Sign-in.

Changing WorldClient's Port Setting

1. Click "Setup » Web & IM Services" on the menu bar.
2. Type the desired port number in the control labeled *Run WorldClient Server using this TCP Port.*
3. Click OK.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

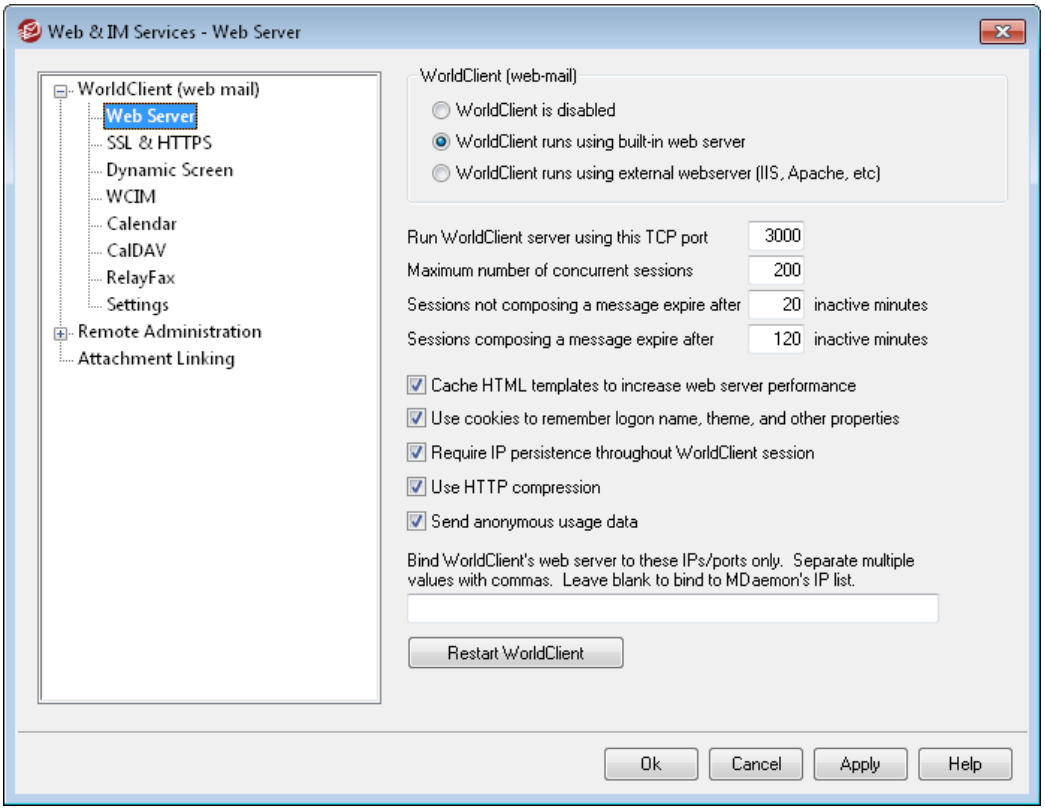
Client-side Help

WorldClient is equipped with extensive client-side help for your users. See the online help system within WorldClient for information on the client features and functions.

For more Address Book options, see:

WorldClient (web mail) » WCIM 239
LDAP 106
Windows Address Book 635

3.6.1.2 Web Server



This screen contains various global, server level settings that govern WorldClient's configuration and behavior regardless of the users or domains to which they belong.

WorldClient (web mail)

WorldClient is disabled
Choose this option to disable WorldClient. You can also toggle WorldClient active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

WorldClient must be active when using the Attachment Linking 262 feature.

WorldClient runs using built-in web server
Choose this option to run WorldClient using MDaemon's built-in web server. You can also toggle WorldClient active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

WorldClient runs using external web server (IIS, Apache, etc)
Choose this option when you wish to run WorldClient under Internet Information Server (IIS) or some other web server instead of MDaemon's built-in server. This prevents certain GUI elements from being accessed which might otherwise cause conflicts with your alternate server.

For more information, see Running WorldClient under IIS 231

Run WorldClient server using this TCP port
This is the port on which WorldClient will listen for connections from your users' web browsers.

Maximum number of concurrent sessions
This is the maximum number of sessions that may be connected to WorldClient at the same time.

Sessions not composing a message expire after xx inactive minutes
When a user is logged in to WorldClient but is not composing a message, this is the amount of time that their session will remain inactive before WorldClient will close it.

Sessions composing a message expire after xx inactive minutes
This timer governs how long a user's session will be kept open while they are composing a message and the session remains inactive. It is a good idea to set this timer higher than the *Sessions not composing a message...* timer, since inactivity time is typically greater while a user is composing a message. This is because composing a message requires no communication with the server until the message is sent.

Cache HTML templates to increase web server performance
Click this box to cause WorldClient to cache templates in memory rather than read them each time they need to be accessed. This can dramatically increase server performance but WorldClient will have to be restarted if you ever make a change to one of the template files.

Use cookies to remember logon name, theme, and other properties
Click this option if you want WorldClient to store each user's logon name, theme, and certain other properties in a cookie on his or her local computer. Using this feature gives your users a more "customized" login experience but requires that they have support for cookies enabled in their browsers.

Require IP persistence throughout WorldClient session
As an added security measure you can click this checkbox to cause WorldClient to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

restrict each user session to the IP address from which the user connected when the session began. Thus, no one can "steal" the user's session since IP persistence is required. This configuration is more secure but could cause problems for users who may be using a proxy server or Internet connection that dynamically assigns and changes IP addresses.

Use HTTP Compression
Click this check box if you want to use HTTP compression in your WorldClient sessions.

Send anonymous usage data
By default WorldClient sends anonymous, benign usage data such as: the OS used, browser version used, language, and the like. This data is used by Alt-N Technologies to help us improve WorldClient. Disable this option if you do not wish to send anonymous usage data.

Bind WorldClient's web server to these IPs/ports only
If you wish to restrict the WorldClient server to only certain IP addresses or ports then specify those IPs and ports here separated by commas. Use the format: "`IP_address:Port`" to designate a port (for example, `192.0.2.0:80`). If you do not include a port, then the default TCP port specified above and the default HTTPS port specified on the SSL & HTTPS 234 screen will be used. Use "`*`" if you want WorldClient to listen on all ports. For example, "`*,*:80`" would cause WorldClient to listen on all IP addresses, on the default ports specified (3000 and 443), and it would also listen on all IP addresses on port 80. If you leave this field blank then WorldClient will monitor all IP addresses designated for your Domains 121.

Restart WorldClient (required when port or IIS value changes)
Click this button if you wish to restart the WorldClient server. Note: when changing WorldClient's port setting you must restart WorldClient in order for the new setting to be recognized.

3.6.1.2.1 Running WorldClient under IIS6

WorldClient is equipped with a built-in web server and therefore doesn't require Internet Information Server (IIS) to operate. However, WorldClient does support IIS, and can therefore function as a ISAPI DLL. The following information on how to configure WorldClient to operate under IIS6 was taken from article #01465 of the MDaemon Knowledge Base at www.altn.com:

1. Open the Internet Information Services Management Console.
2. Right-Click on **Application Pools**.
3. Choose **New/Application Pool**.
4. Name the Pool **Alt-N** and click the **OK** button.
5. Right-Click on **Alt-N**.
6. Click on **Properties**.
7. Click on the **Performance** tab.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

8. Uncheck the options for **Shutdown worker processes after being idle for (time in minutes):** and **Limit the kernel request queue (number of requests)**.
9. Click on the **Identity** tab.
10. In the drop-down for Predefined, choose **Local Service**.
11. Click the **OK** button.
12. Right-Click on **Web Sites**.
13. Choose **New**.
14. Click on **Web Site**. (This will launch a wizard)
15. Click on the **Next** button.
16. Type in a name for the site such as **WorldClient**.
17. Click on the **Next** button.
18. Click on the **Next** button again.
19. Browse to the Home directory: which will be **C:\MDaemon\WorldClient\HTML** with a default installation.
20. Click on the **Next** button.
21. Make sure the options for **Read**, **Run Scripts**, and **Execute** are checked.
22. Click on the **Next** button.
23. Click on the **Finish** button.
24. Right click on the website you just made **(WorldClient)**.
25. Choose **Properties**.
26. Click on the **Documents** tab.
27. Remove all listed documents.
28. Add **WorldClient.dll**.
29. Choose the **Home Directory** tab.
30. Choose **Alt-N** in the Application Pool drop-down.
31. Click the **OK** button.
32. Click on **Web Service Extensions**.
33. Enable **All Unknown ISAPI Extension** or Create a new one for **WorldClient.DLL**.

The Internet Guest Account - **IUSER_<SERVER_NAME>** - needs **Full Access** NTFS permissions for the MDaemon directory and all sub-directories.

1. Right-Click on the MDaemon directory. (C:\MDaemon)
2. Select **Properties**.
3. Select the **Security** tab.
4. Click the **Add** button.
5. Click the **Advanced** button.
6. Click the **Find Now** button.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

7. Select **IUSER_<SERVER_NAME>** (where "<SERVER_NAME>" is the name of the local computer).
8. Click the **OK** button.
9. Click the **OK** button.
10. Check the box for **Full Control**.
11. Click the **OK** button.

These same steps need to be applied to any directory MDaemon is configured to use.

When doing upgrades to MDaemon after setting up the web:

1. Open the Internet Information Services Management Console.
2. Open **Application Pool** list.
3. Right-Click **Alt-N**.
4. Choose **Stop**.
5. Shutdown MDaemon.
6. Install the upgrade.
7. Once installation is complete, start MDaemon.
8. In Information Services Management Console again, Right-Click **Alt-N**.
9. Choose **Start**.

If you follow the above method, the following should occur.

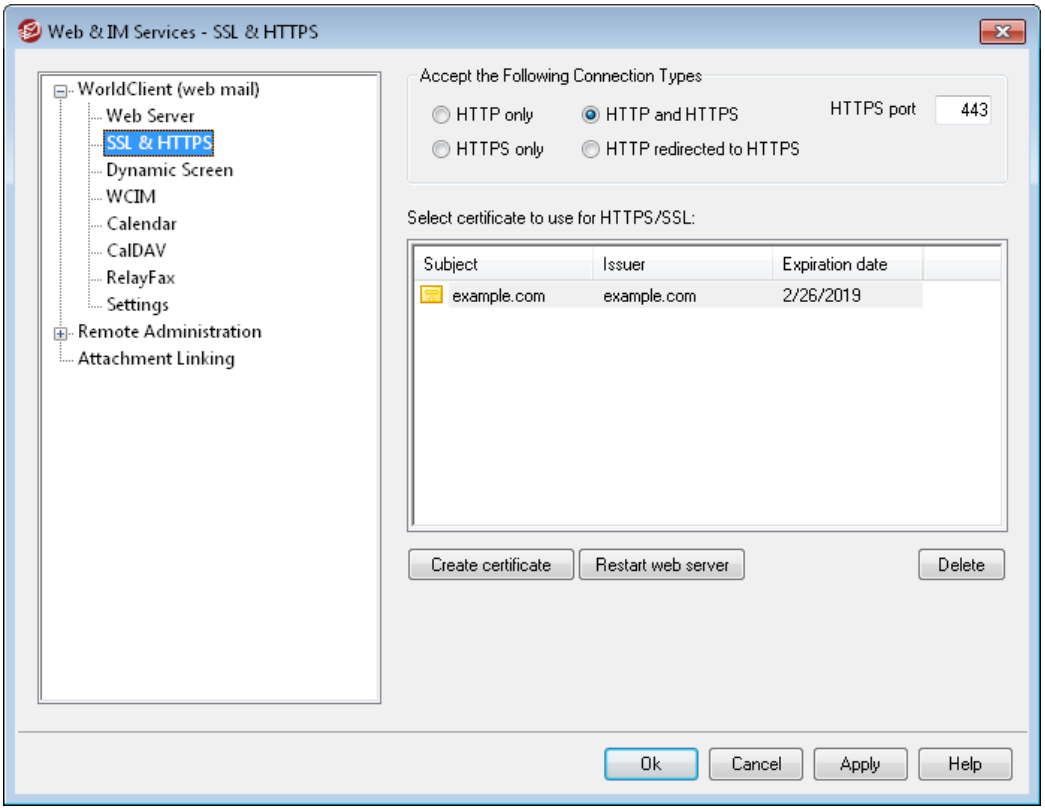
1. After stopping the **Application Pool** users will get a message **Service Unavailable**.
2. Following these steps should help minimize your chances of having to reboot your computer after upgrading MDaemon.

The setup of this program under IIS is NOT supported by tech support and those who choose to run WC under IIS must be aware of all security issues and ramifications of running any applications under IIS. It is recommended that all Patches and updates be installed on IIS before the installation of WorldClient as an ISAPI extension.

When running WorldClient under IIS you will no longer be able to start and stop it from MDaemon's interface. You must use the tools provided with IIS to do so.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.6.1.3 SSL & HTTPS



MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. SSL is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring WorldClient to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » WorldClient (web mail)". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » WorldClient".

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 487

This screen only applies to WorldClient when using MDaemon's built-in web server. If you configure WorldClient to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

Accept the Following Connection Types

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

HTTP only
Choose this option if you do not wish to allow any HTTPS connections to WorldClient. Only HTTP connections will be accepted.

HTTP and HTTPS
Choose this option if you want to enable SSL support within WorldClient, but do not wish to force your WorldClient users to use HTTPS. WorldClient will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the WorldClient TCP port designated on the Web Server 229 screen of WorldClient (web mail).

HTTPS only
Choose this option if you wish to require HTTPS when connecting to WorldClient. WorldClient will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

HTTP redirected to HTTPS
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

HTTPS port
This is the TCP port that WorldClient will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in WorldClient's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the WorldClient port that is designated on the Web Server 229 screen of WorldClient (web mail). If you are still allowing HTTP connections to WorldClient then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

Select certificate to use for HTTPS/SSL

This box displays your SSL certificates. Click a certificate to designate it as the one WorldClient will use. Double-click a certificate to open it in the Certificate dialog for review.

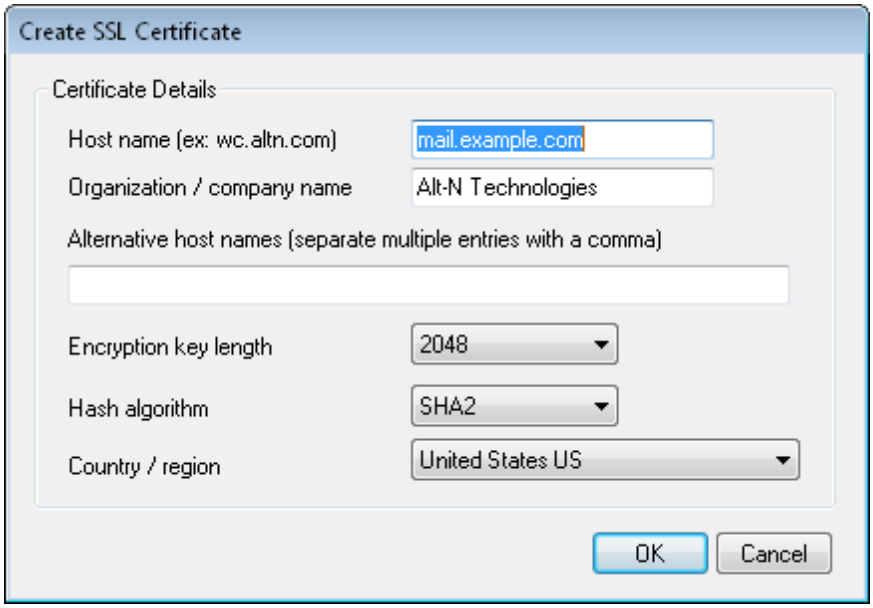
MDaemon does not support multiple certificates for WorldClient. All WorldClient domains must share a single certificate. If you have more than one WorldClient domain then enter those domain names (and any others that you wish to use to access WorldClient) into the option called "*Alternative host names (separate multiple entries with a comma)*" outlined below.

Delete
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Host name
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

Organization/company name
Enter the organization or company that "owns" the certificate here.

Alternative host names (separate multiple entries with a comma)
MDaemon does not support multiple certificates — all WorldClient domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Country/region
Choose the country or region in which your server resides.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

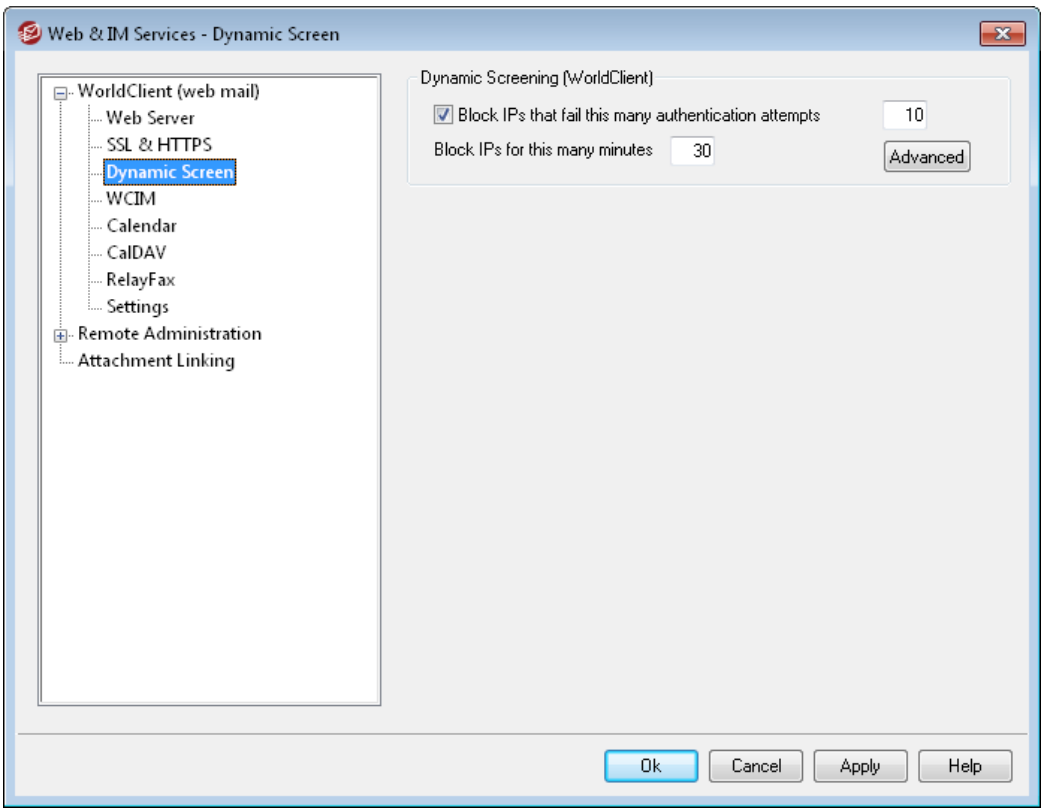
Restart web server

Click this button to restart the web server. The web server must be restarted before a new certificate will be used.

See:

SSL & Certificates 487
Creating and Using SSL Certificates 500

3.6.1.4 Dynamic Screen



Dynamic Screening (WorldClient)

Block IPs that fail this many authentication attempts
Use this option if you wish to temporarily block IP addresses that fail a WorldClient authentication attempt a specified number of times. This can help prevent attempts to "hack" a user account and falsely authenticate a session. This option monitors only WorldClient connections.

WorldClient sends an email to the postmaster when dynamic screening bans an IP address. The following settings to control this option are located in the `WorldClient.ini` file at:

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

```
\MDaemon\WorldClient\WorldClient.ini

[DynamicScreening]
SendBanNotification=Yes
SendBanNotificationTo=postmaster
```

Block IPs for this many minutes
When an IP address is automatically blocked, this is the number of minutes the block will last. When the block expires the IP address will be able to connect to you again normally. This feature prevents you from accidentally blocking a valid IP address permanently.

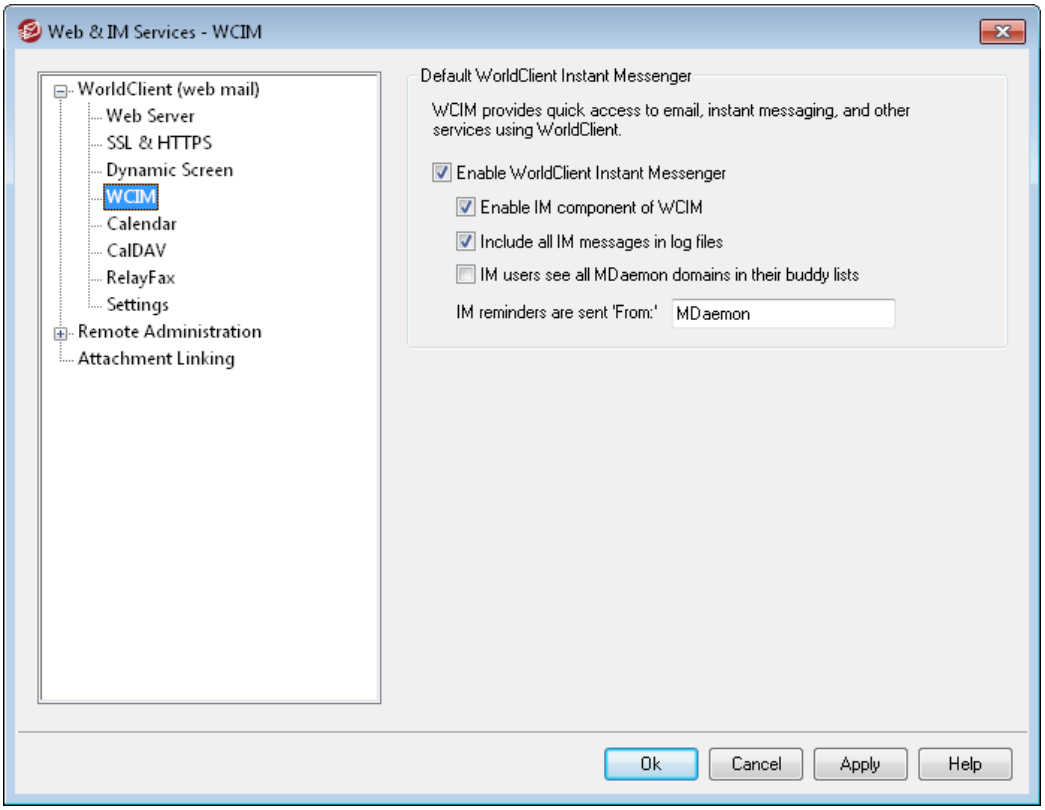
Advanced
Click this button to open the Dynamic Screen's WorldClient block list. This lists all IP addresses that have been blocked from connecting to WorldClient. You can manually add IP addresses and the number of minutes to block them by listing them one entry per line in the form: `IP_address<space>Minutes`. For example, `192.0.2.0 60`.

See:

Domain Manager » WorldClient Instant Messenger 130
Account Editor » Web Services 526
Group Properties 577

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.6.1.5 WCIM



This screen controls the default settings of new domains for WorldClient Instant Messenger (WCIM) 225. Settings for specific domains can be modified via the Domain Manager's WorldClient Instant Messenger screen 130. WorldClient Instant Messenger services can be enabled or disabled for specific accounts or groups via the Web Services 526 and Group Properties 577 screens respectively.

Default WorldClient Instant Messenger

Enable WorldClient Instant Messengert
Enable this option if you wish to make WorldClient Instant Messenger available to a domain's users by default. They can download it from the Options » WorldClient Instant Messenger page within WorldClient. The downloaded installation file will be automatically customized for each user's account to make installation and setup easier.

Enable IM component of WCIM
Click this option if you want to activate WCIM's instant messaging (IM) system for a domain's users by default. Clear the check box if you want the IM controls to be unavailable.

Include all IM messages in log files
Click this check box if by default you want all of a domain's instant messaging traffic to be included in the `InstantMessaging.log` file (located in the `MDaemon/LOGS/` folder).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

IM users see all MDaemon domains in their buddy lists
Click this option if by default you want users of a new domain to be able to add users to their buddy lists from all of your MDaemon domains, instead of only being able to add users from their own domain. Clear this checkbox if you want only users of the same domain to be available for adding to buddy lists. For example, if your MDaemon is hosting mail for example.com and example.org, then activating this control for your example.com users will enable them to add buddies to their lists from both domains. Clearing it would mean that they could only add other example.com users.

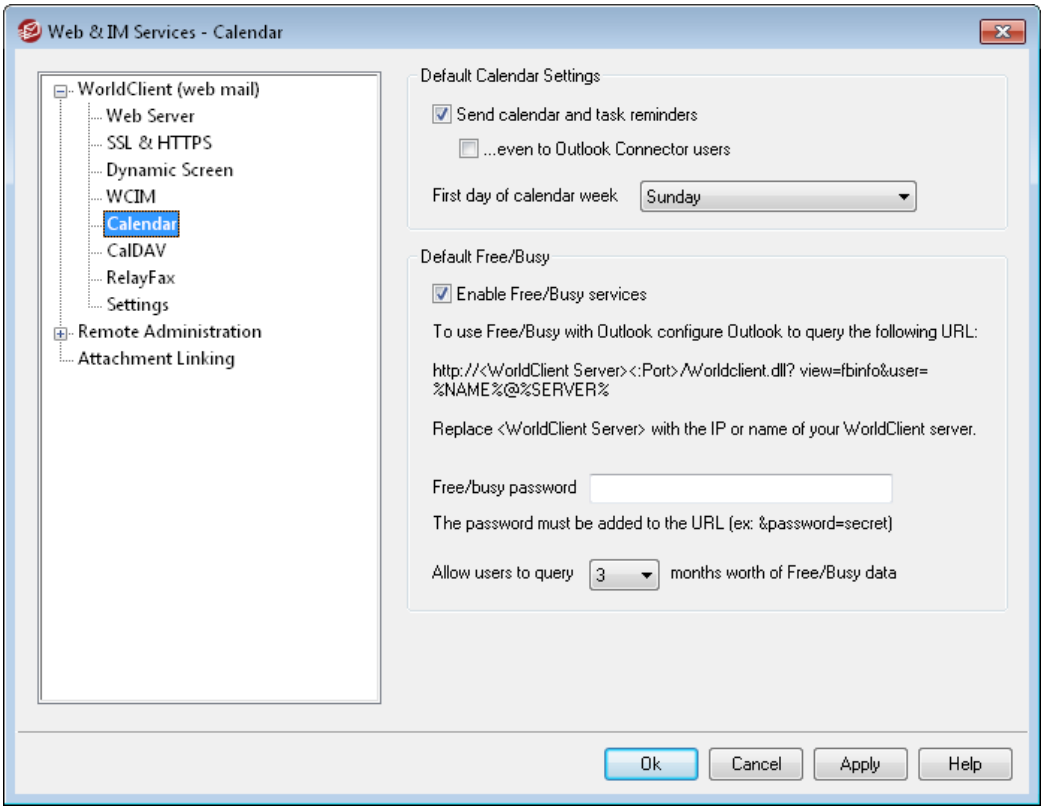
IM reminders are sent 'From:'
When an appointment is scheduled on a user's WorldClient calendar, the event can be set to send a reminder to the user at a specified time. If the IM system is active for the user's domain then the reminder will be sent in an instant message if he or she is using WCIM. Use this text box to specify the name that you wish the message to appear to be '`From:`'. This is the default setting for new domains. You can change it for specific domains via the Domain Manager's WorldClient Instant Messenger screen 130..

See:

Domain Manager » WorldClient Instant Messenger 130
Account Editor » Web Services 526
Group Properties 577

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.6.1.6 Calendar



This screen controls the default settings for MDaemon's Calendar features. Settings for specific domains can be controlled via the Domain Manager's Calendar 132 screen.

Default Calendar Settings

Send calendar and task reminders
Click this checkbox if you wish to allow WorldClient's calendar and task reminders to be sent to your users via email and WorldClient Instant Messenger.

...even to Outlook Connector users
If you have enabled the "*Send calendar and task reminders*" option above, click this option if you also wish to enable reminders for Outlook Connector users.

First day of week
Choose a day from the drop-down list. The selected day will appear in the calendars as the first day of the week.

Default Free/Busy

MDaemon includes a Free/Busy server, which makes it possible for a meeting planner to view the availability of potential meeting attendees. To access this feature, click Scheduling within WorldClient when creating a new appointment. This opens a Scheduling window containing the list of attendees and a color-coded calendar grid with a row for each one. Each attendee's row is color-coded to indicate the times at

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

which he or she might be available for a meeting. There are colors for Busy, Tentative, Out of Office, and No information. There is also an Auto-Pick Next button that makes it possible for you to query the server for the next time slot at which all attendees may be available. When you have finished creating the appointment it will send an invitation to all of the attendees, who can then accept or decline.

WorldClient's Free/Busy server is also compatible with Microsoft Outlook. To use it, configure Outlook to query the URL listed below for Free/Busy data. In Outlook 2002, for example, the Free/Busy options are located under "Tools » Options » Calendar Options... » Free/Busy Options..."

Free/Busy server URL for Outlook:

```
http://<WorldClient><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%
@%SERVER%
```

Replace "<WorldClient>" with the IP address or domain name of your WorldClient server, and "<:Port>" with the port number (if you aren't using the default web port). For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

For more on how to use WorldClient's Free/Busy features to schedule your appointments, see the online Help system within WorldClient.

Enable Free/Busy services
Click this option if you wish to provide access to the Free/Busy server features to users.

Free/Busy password
If you wish to require a password when users attempt to access the Free/Busy server features via Outlook, include the password here. This password must be appended to the URL listed above (in the form: "&password=FBServerPass") when the users configure their Free/Busy settings within Outlook. For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%&password=MyFBServerPassword
```

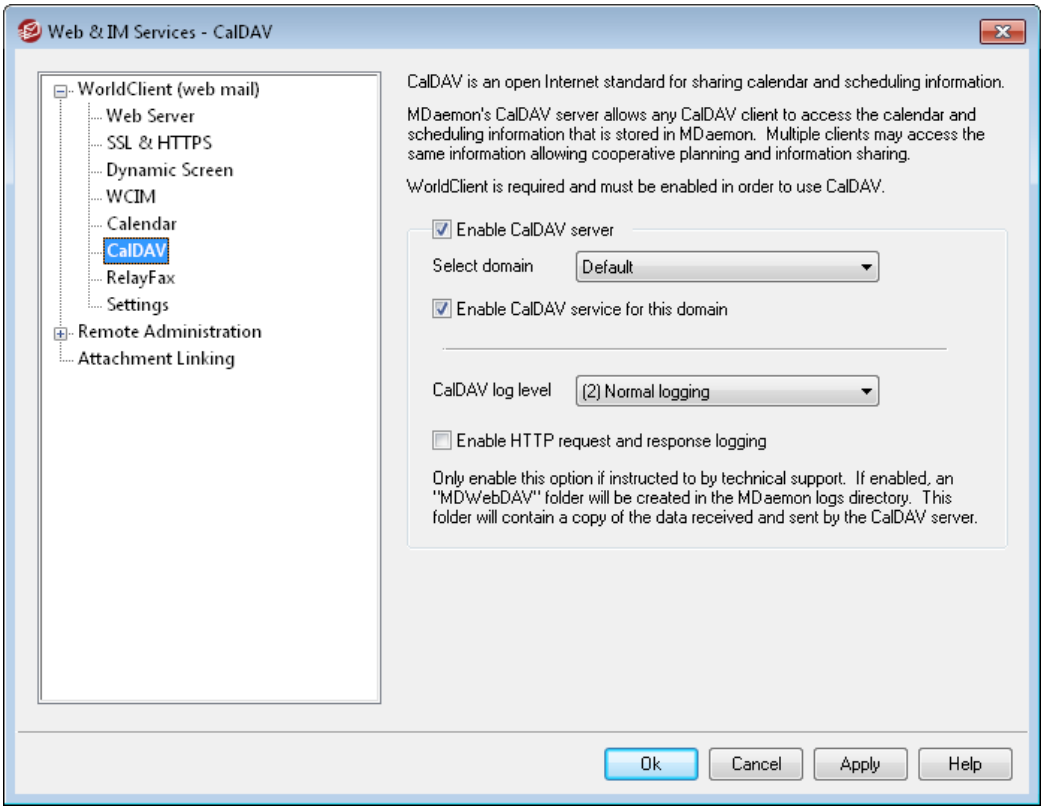
Allow users to query X months worth of Free/Busy data
Use this option to designate how many months worth of Free/Busy data your users may query.

See:

Domain Manager » Calendar 132

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.6.1.7 CalDAV


Web & IM Services - CalDAV
WorldClient (web mail)
Web Server
SSL & HTTPS
Dynamic Screen
WCIM
Calendar
CalDAV
RelayFax
Settings
Remote Administration
Attachment Linking
CalDAV is an open Internet standard for sharing calendar and scheduling information.
MDaemon's CalDAV server allows any CalDAV client to access the calendar and scheduling information that is stored in MDaemon. Multiple clients may access the same information allowing cooperative planning and information sharing.
WorldClient is required and must be enabled in order to use CalDAV.
Enable CalDAV server
Select domain
Default
Enable CalDAV service for this domain
CalDAV log level
(2) Normal logging
Enable HTTP request and response logging
Only enable this option if instructed to by technical support. If enabled, an "MDWebDAV" folder will be created in the MDaemon logs directory. This folder will contain a copy of the data received and sent by the CalDAV server.
Ok
Cancel
Apply
Help

CalDAV is an Internet standard for managing and sharing calendars and scheduling information. MDaemon's CalDAV support makes it possible for your accounts to use any client that supports CalDAV to access and manage their personal calendars and tasks. They can also access any public 218 or shared 547 calendars or tasks according to their access rights 220.

Enable CalDAV
CalDAV support is enabled by default. However, WorldClient is required for CalDAV and therefore must be enabled 229 in order to use it. Disable this option if you do not wish to support CalDAV. To enabled/disable CalDAV for individual domains, use the options below.

Changing the Default CalDAV Setting for Domains
Initially, all of MDaemon's domains will have CalDAV enabled or disabled based the *Default* selection in the *Select domain* drop-down list. To change the default setting:

1. In the *Select domain* drop-down list, choose **Default**.
2. Check the box next to **Enable CalDAV service for this domain** if you want CalDAV to be enabled for all domains by default, or clear the box if you want it to be disabled by default.
3. Click **Ok**.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Enabling/Disabling CalDAV for Specific Domains

To override the *Default* CalDAV setting for individual domains:

1. In the *Select domain* drop-down list, choose a specific domain.
2. Check the box next to **Enable CalDAV service for this domain** if you want CalDAV to be enabled for the domain, or clear the box if you want it to be disabled.
3. Click **OK**.

Logging

CalDAV log level

Use this drop-down list to designate the degree to which CalDAV activities will be logged. There are six possible levels of logging: 1-Debug logging, 2-Normal logging (default), 3-Warnings and errors only, 4-Errors only, 5-Critical errors only, and 6-No logging. This is a global setting—it cannot be applied to specific domains

Enable HTTP request and response logging

If enabled, this will create an `MDWebDAV` folder in MDaemon's logs folder. All data sent and received by the CalDAV server will be logged to that folder. Ordinarily this option would only be used for diagnostics and shouldn't be enabled unless you are instructed by Technical Support to do so.

Configuring CalDAV Clients

To configure clients that support RFC 6764 (Locating Services for Calendaring Extensions to WebDAV (CalDAV)), only the server, user name, and password should be required. You can setup your DNS records to point the client to the correct URL. When a DNS record has not been configured, the user can enter a special "well-known URL" in the client: "hostname/.well-known/caldav". For example: `http://example.com:3000/.well-known/caldav` . WorldClient's built-in web server support the well-known URL.

Clients that do not support automatically locating the CalDAV service, such as Mozilla Thunderbird via the Lightning plugin, will require a full URL for each Calendar and Task list. MDaemon's CalDAV URLs are constructed like this:

Calendars and Tasks

User's default calendar or task list:

`http://[host]/webdav/calendar`
(e.g. `http://example.com:3000/webdav/calendar`)

`http://[host]/webdav/tasklist`
(e.g. `http://example.com/webdav/tasklist`)

User's custom calendar or task list:

`http://[host]/webdav/calendar/[calendar-name]`
(e.g. `http://example.com/webdav/calendar/personal`)

`http://[host]/webdav/tasklist/[tasklist-name]`
(e.g. `http://example.com/webdav/tasklist/todo`)

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

User's custom calendar or task list in a subfolder:

http://[host]/webdav/calendar/[folder]/[calendar-name]
(e.g. `http://example.com/webdav/calendar/my-stuff/personal`)

http://[host]/webdav/tasklist/[folder]/[tasklist-name]
(e.g. `http://example.com/webdav/tasklist/my-stuff/todo`)

Shared Calendars and Tasks
Another user's default calendar or task list:

`http://[host]/webdav/calendars/[domain]/[user]`
(e.g. `http://example.com/webdav/calendars/example.net/frank`)

`http://[host]/webdav/tasks/[domain]/[user]`
(e.g. `http://example.com/webdav/tasks/example.net/frank`)

Another user's custom calendar or task list:

`http://[host]/webdav/calendars/[domain]/[user]/[calendar-name]`
(e.g. `http://example.com/webdav/calendars/example.net/frank/personal`)

`http://[host]/webdav/tasks/[domain]/[user]/[tasklist-name]`
(e.g. `http://example.com/webdav/tasks/example.net/frank/todo`)

Public Calendars and Tasks
Domain's default calendar or task list:

`http://[host]/webdav/public-calendars/[domain]`
(e.g. `http://example.com/webdav/public-calendars/example.com`)

`http://[host]/webdav/public-tasks/[domain]`
(e.g. `http://example.com/webdav/public-tasks/example.com`)

Calendar or task list in the root of the Public Folder hierarchy:

`http://[host]/webdav/public-calendars/[calendar-name]`
(e.g. `http://example.com/webdav/public-calendars/holidays`)

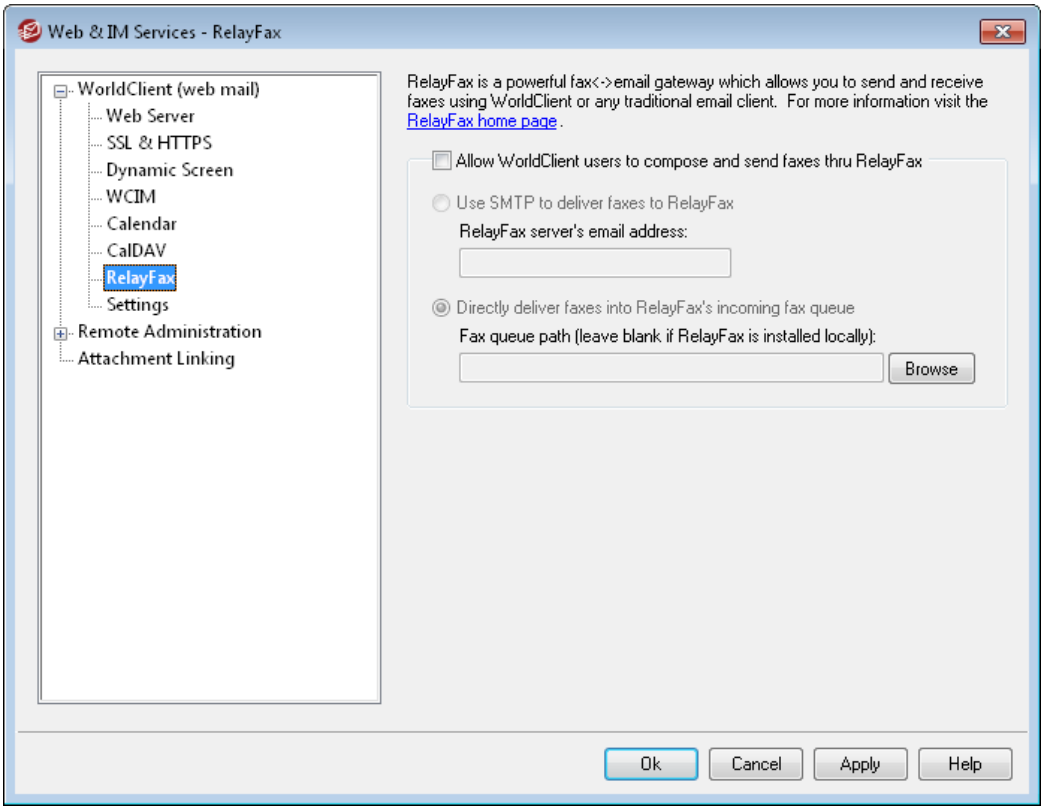
`http://[host]/webdav/public-tasks/[tasklist-name]`
(e.g. `http://example.com/webdav/public-tasks/projects`)

Special care should be taken if testing the OutlookDAV client. If multiple MAPI profiles exist we've seen the client issue delete commands to the server for all of the calendar items returned by the server. OutlookDAV only supports the default MAPI profile.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

For more information on setting up CalDAV clients, see CalDAV Client Setup at altn.com.

3.6.1.8 RelayFax


Web & IM Services - RelayFax
WorldClient (web mail)
Web Server
SSL & HTTPS
Dynamic Screen
WCIM
Calendar
CalDAV
RelayFax
Settings
Remote Administration
Attachment Linking
RelayFax is a powerful fax<->email gateway which allows you to send and receive faxes using WorldClient or any traditional email client. For more information visit the RelayFax home page.
Allow WorldClient users to compose and send faxes thru RelayFax
Use SMTP to deliver faxes to RelayFax
RelayFax server's email address:
Directly deliver faxes into RelayFax's incoming fax queue
Fax queue path (leave blank if RelayFax is installed locally):
Browse
Ok
Cancel
Apply
Help

Alt-N Technologies' RelayFax Server is an email to fax and fax to email gateway that can be seamlessly integrated with WorldClient in order to provide its services to your users. When this functionality is enabled, WorldClient users will be given access to various features that will enable them to compose and send faxes via the WorldClient client pages. For more information, visit the RelayFax section of www.altn.com.

RelayFax Integration Options

Allow WorldClient users to compose and send faxes thru RelayFax
Click this option to integrate RelayFax with WorldClient. When active it will cause a "Compose Fax" control and other fax related features to appear on the WorldClient pages.

Use SMTP to deliver faxes to RelayFax
RelayFax monitors a specific mailbox for incoming messages that are to be faxed. Click this option and MDaemon will use the normal SMTP email delivery process to send these messages to that mailbox's address. This option is useful when RelayFax

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

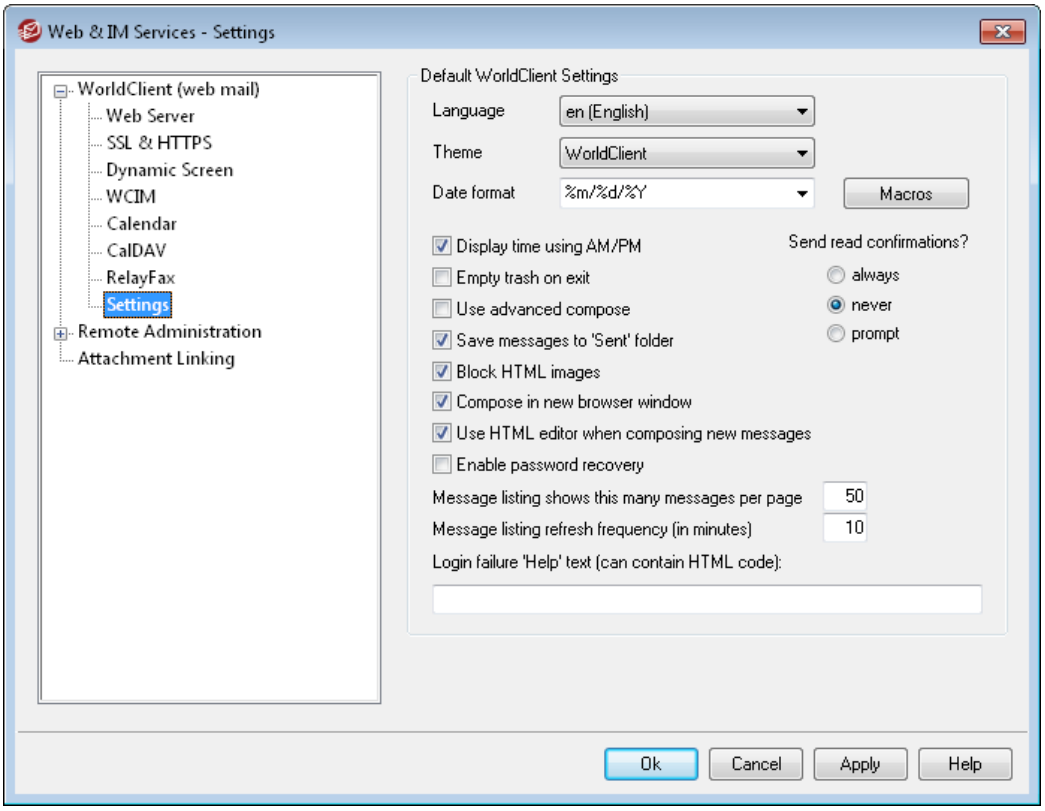
is monitoring a mailbox located somewhere other than your local network. If RelayFax resides on your network you may choose to have MDaemon deliver the messages directly to RelayFax's message queue and thus bypass the SMTP delivery process altogether. For more information on this method, see *Directly deliver faxes into RelayFax's incoming fax queue* below.

RelayFax server's email address
Specify the email address to which you want messages intended for faxing to be delivered. This value must match the address that you have configured RelayFax to monitor for these messages.

Directly deliver faxes into RelayFax's incoming fax queue
If RelayFax resides on your LAN you may choose this method rather than SMTP for distributing messages for faxing. When MDaemon receives a message intended for RelayFax it will be placed directly into RelayFax's incoming queue rather than delivered using SMTP.

Fax queue path
If RelayFax resides on the same machine on which MDaemon is running, you may leave this file path blank. Otherwise, you must specify the network path to RelayFax's \app\ folder.

3.6.1.9 Settings



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

This screen designates the default settings for the Domain Manager's WorldClient Settings 134 screen. When a user signs in to WorldClient, these options govern how various WorldClient features initially work for that user. Many of these settings can then be customized by the user via the Options pages within WorldClient.

Default WorldClient Settings

Language
Use the drop-down list box to choose the default language in which the WorldClient interface will appear when your users first sign in to the selected domain. Users can change their personal language setting on the WorldClient Sign-in page, and through an option in Options » Personalize within WorldClient.

Theme
Use this drop-down list box to designate the default WorldClient theme to used for users whenever they sign in for the first time. The users can personalize the theme setting from Options » Personalize within WorldClient.

Date format
Use this text box to designate how dates will be formatted within WorldClient. Click the *Macros* button to display a list of macro codes that can be used in this text box. You can use the following macros in this control:

%A — Full weekday name

%B — Full month name

%d — Day of month (displays as "01-31")

%m — Month (displays as "01-12")

%y — 2-digit year

%Y — 4-digit year

For example, "`%m/%d/%Y`" might be displayed in WorldClient as "`12/25/2011`".

Macros
Click this button to display the list of macro codes that can be used in the *Date format*.

Display time using AM/PM
Click this option if you want a 12-hour clock with AM/PM to be used within WorldClient for times displayed. Clear the check box if you want to use a 24-hour clock. Individual users can modify this setting via the "*Display my hours in an AM/PM format*" option located on the Options » Calendar page within WorldClient.

Empty trash on exit
This option causes the user's trash to be emptied when he or she signs out from WorldClient. Individual users can modify this setting from the Options » Personalize page within WorldClient.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Use advanced compose
Check this box if you want users to see the Advanced Compose screen in WorldClient rather than the normal Compose screen by default. Individual users can modify this setting from Options » Compose within WorldClient.

Save messages to 'Sent' folder
Click this option if you want a copy of each message that you send to be saved in your mailbox's *Sent* folder. Individual users can modify this setting from the Options » Compose page within WorldClient.

Block HTML images
Enable this check box if you wish to prevent remote images from being displayed automatically when viewing HTML email messages in WorldClient. In order to view the images the user must click the bar that appears above the message in the browser window. This is a spam prevention feature, because many spam messages contain images with special URLs that identify the email address of the user who viewed the images, thus confirming to the spammer that it is a valid, working address. This option is enabled by default.

Compose in new browser window
Check this box if you want a separate browser window to open for composing messages instead of simply switching the main window to the compose screen. Clear the box if you do not want separate windows to open. Individual users can modify this setting from the Options » Compose page within WorldClient.

Use HTML editor when composing new messages
Check this box if you want users to see the HTML compose editor by default in WorldClient. They can control this setting for themselves from Options » Compose within WorldClient.

Enable password recovery
If enabled, users who have permission to edit their password 526 will be able to enter an alternate email address in WorldClient, which can be sent a link to reset their password if they forget it. To set up this feature, users must enter both the password recovery email address and their current password in WorldClient on the Options » Personalize page. Once set, if the user attempts to log in to WorldClient with an incorrect password a "forgot password?" link will appear. This link takes them to a page that asks them to confirm their password recovery email address. If entered correctly, an email will be sent with a link to a change password page. This feature is disabled by default.

You can enable or disable this option on a per-user basis by adding the following key to a WorldClient user's `user.ini` file (e.g. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (or "=No" to disable the option for the
user)
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Send read confirmations?
This option governs how WorldClient will respond to incoming messages that contain a request for read confirmation.

always
If this option is selected, MDaemon will send a notification to the sender indicating that the message was read. The WorldClient user who received the message will not see any indication that the read confirmation was requested or responded to.

never
Choose this option if you want WorldClient to ignore read confirmation requests.

prompt
Select this option if you wish to ask WorldClient users whether or not to send a read confirmation each time a message is opened that requests it.

Message listing shows this many messages per page
This is the number of messages that will be listed on each page of the Message Listing for each of your mail folders. If a folder contains more than this number of messages then there will be controls above and below the listing that will allow you to move to the other pages. Individual users can modify this setting from Options » Personalize within WorldClient.

Message listing refresh frequency (in minutes)
This is the number of minutes that WorldClient will wait before automatically refreshing the Message Listing. Individual users can modify this setting from Options » Personalize within WorldClient.

Login failure 'Help' text (can contain HTML code)
You can use this option to specify a sentence of text (either plain text or HTML) to display on the WorldClient sign-in page when a user encounters a problem signing in. The text is displayed below the following default text: "*Incorrect Logon, please try again. If you need assistance please contact your email administrator.*" This text could be used to direct users to a page or contact info for help regarding signing in to WorldClient.

See:

Domain Manager » WorldClient Settings 134

3.6.1.10 Branding

If you wish to customize the WorldClient banner images that appear on the login page and in the navigation sidebar, you can do so from the Branding page in MDaemon's Remote Administration 251 web interface.

To use your own custom images:

1. Click **Use custom images** in the Customization section.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

2. In the Login Page Image section, use the **Choose File** or **Browse** option (depending on your browser) to select the file you wish to upload. WorldClient's default login page image is 382x88 pixels.
3. Click **Upload Custom Image**.
4. Repeat steps 2 and 3 for the Navigation Sidebar Image. WorldClient's default sidebar image is 191x44 pixels.

The uploaded images will appear in their corresponding boxes and now be used instead of WorldClient's default images.

3.6.2 Remote Administration

MDaemon's Remote Administration web interface is designed to make it possible for you to administer MDaemon remotely using a web browser. It is a server application designed to run in the background on the same computer as MDaemon. To access Remote Administration, open your browser to the URL and port number on which the remote administration server resides (e.g. `www.example.com:1000`). After providing your login credentials, you will be given access to various controls and settings within MDaemon. The type and number of settings to which you will have access is dependent upon the level of access given. There are three levels of access that can be provided to remote administration users: Global, Domain, and User.

Global Administrators — Global administrators are users who have global access permission enabled under their account settings within MDaemon. Global access means that the user can see and configure every setting and control that is accessible via Remote Administration. Global administrators can add, edit, and delete users, domains, and mailing lists. They can edit product INI files, designate other users as Domain administrators, manage passwords, and do many other things; they have complete administrative control.

Domain Administrators — Similar to Global administrators, Domain administrators also have control over the users and settings accessible via Remote Administration. Their administrative control, however, is limited to the domain or domains to which they have been given access and the permissions designated on the Web Services 526 screen. Domain administrators and the domains over which they have control are designated from within Remote Administration by a Global administrator, or by another Domain administrator with access to those domains.

Users — The lowest possible level of Remote Administration access is User access. MDaemon users can sign in to the remote administration interface and, for example, view their individual account settings as well as edit their MultiPOP entries, mail filters, Autoresponders, and so on. The type and number of settings that can be edited depends on the permissions given in each user's account settings

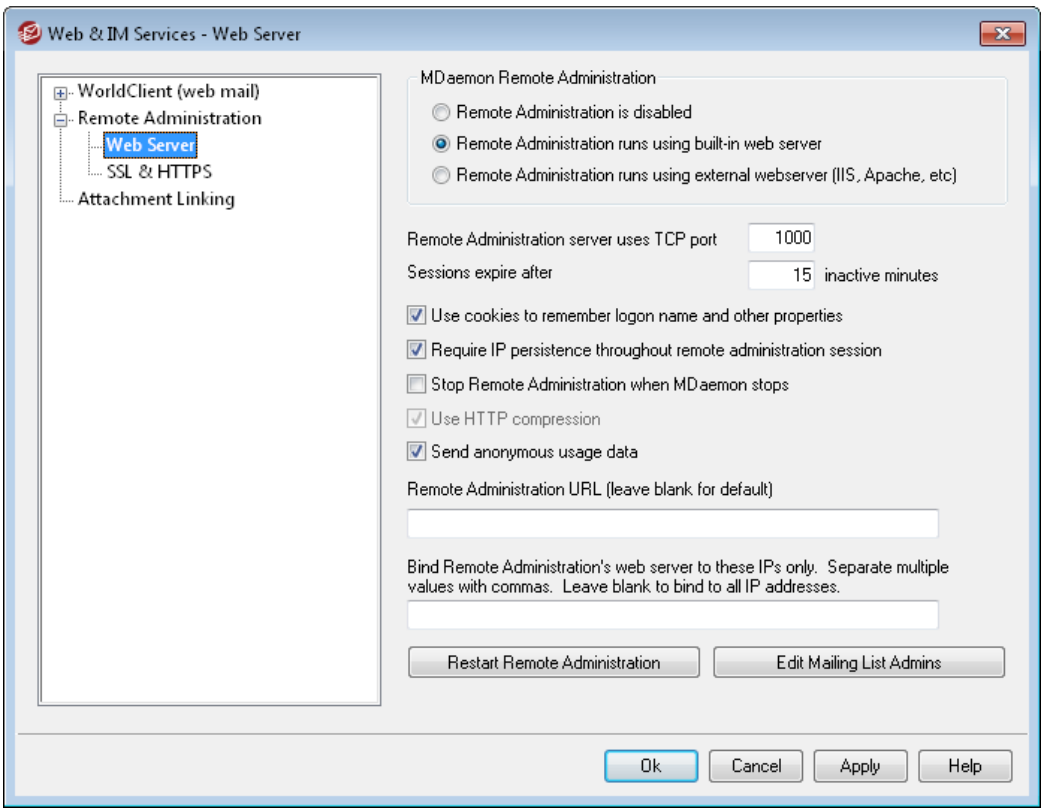
Everyone who has permission to access both WorldClient and Remote Administration can access Remote Administration from within WorldClient, rather than having to sign in to both separately. Remote Administration is opened in a separate browser window from within WorldClient by clicking the "Advanced Settings" link under "Options".

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Remote Administration » Web Server 252
Remote Administration » HTTPS 255
Template Manager » Web Services 587
Account Editor » Web Services 526
Running Remote Administration under IIS 258

3.6.2.1 Web Server


Web & IM Services - Web Server
WorldClient (web mail)
Remote Administration
Web Server
SSL & HTTPS
Attachment Linking
MDaemon Remote Administration
Remote Administration is disabled
Remote Administration runs using built-in web server
Remote Administration runs using external webserver (IIS, Apache, etc)
Remote Administration server uses TCP port
1000
Sessions expire after
15
inactive minutes
Use cookies to remember logon name and other properties
Require IP persistence throughout remote administration session
Stop Remote Administration when MDaemon stops
Use HTTP compression
Send anonymous usage data
Remote Administration URL (leave blank for default)
Bind Remote Administration's web server to these IPs only. Separate multiple values with commas. Leave blank to bind to all IP addresses.
Restart Remote Administration
Edit Mailing List Admins
Ok
Cancel
Apply
Help

MDaemon Remote Administration

Remote Administration is disabled
Choose this option to disable Remote Administration. You can also toggle Remote Administration active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

Remote Administration runs using built-in web server
Choose this option to run Remote Administration using MDaemon's built-in web server. You can also toggle Remote Administration active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Remote Administration runs using external web server (IIS, Apache, etc)
Choose this option when you wish to run Remote Administration under Internet Information Server (IIS) or some other web server instead of MDaemon's built-in server. This prevents certain GUI elements from being accessed which might otherwise cause conflicts with your alternate server.

For more information, see Running Remote Administration under IIS 258.

Remote Administration server uses TCP port
This is the port on which Remote Administration will listen for connections from your web browser. The default port is 1000.

Sessions expire after xx inactive minutes
When you are logged in to Remote Administration, this is the amount of time that your session is allowed to be inactive before Remote Administration will close it. The default is 15 minutes.

Use cookies to remember logon name and other properties
Click this option if you want Remote Administration to store your logon name and certain other properties in a cookie on your local computer. Using this feature gives you a more customized login experience but requires that they have support for cookies enabled in your browser.

Require IP persistence throughout remote administration session
As an added security measure you can click this checkbox to cause Remote Administration to restrict each session to the IP address from which you connected when the session began. Thus, no one can "steal" the session since IP persistence is required. This configuration is more secure but could cause problems if you are using a proxy server or Internet connection that dynamically assigns and changes IP addresses.

Stop Remote Administration when MDaemon stops
Click this option if you want Remote Administration to be shut down whenever MDaemon is shut down. Otherwise, Remote Administration will continue to run in the background.

Send anonymous usage data
By default MDaemon's Remote Administration web client sends anonymous, benign usage data such as: the OS used, browser version used, language, and the like. This data is used by Alt-N Technologies to help us improve Remote Administration. Disable this option if you do not wish to send anonymous usage data.

Remote Administration URL
This is the URL that WorldClient will use internally when users click the Advanced Settings link to edit their account settings via Remote Administration. If you are running Remote Administration with the built-in web server, then leave this field blank. If you are using an alternate web server such as IIS, and you have configured Remote Administration to run at an alternate URL or IP address, then specify that URL here.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Bind Remote Administration's web server to these IPs only
If you wish to restrict the remote administration server to only certain IP addresses, specify those addresses here separated by commas. If you leave this field blank then Remote Administration will monitor all IP Addresses that you have designated for your Domains 121.

Restart Remote Administration (required when port or IIS value changes)
Click this button if you wish to restart the remote administration server. Note: when changing the port setting you must restart Remote Administration in order for the new setting to be recognized.

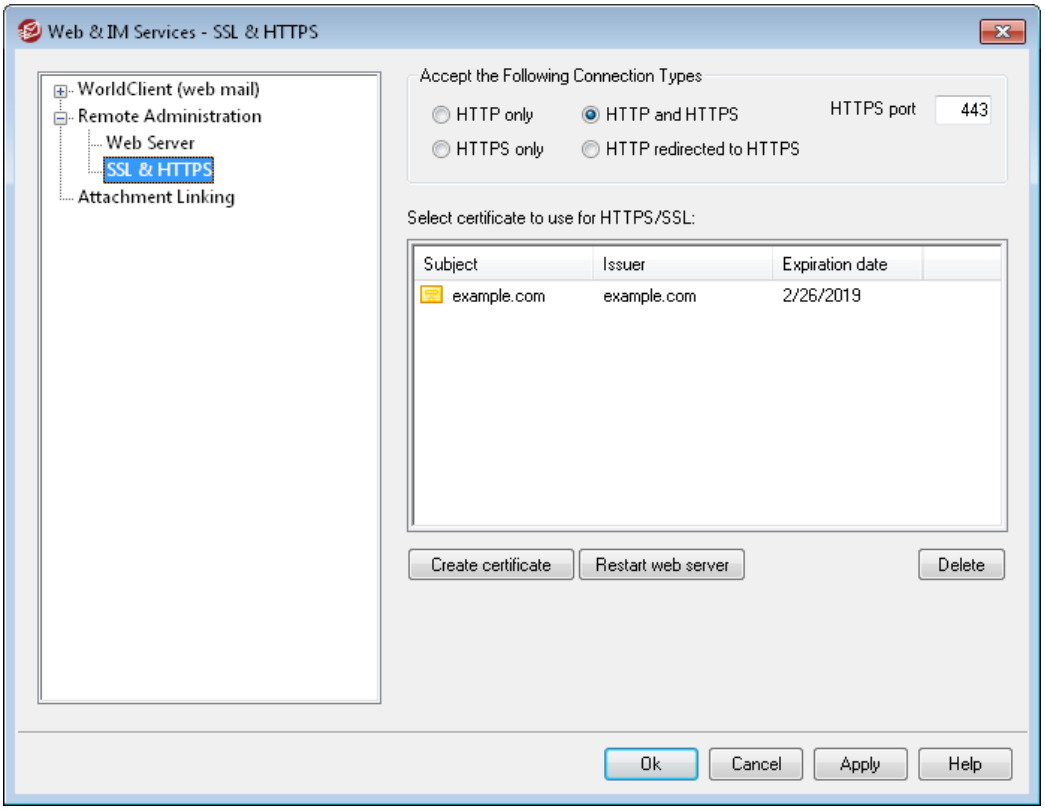
Edit Mailing List Admins
Click this button if you wish to open the mailing list administrators file to view or edit it.

See:

Remote Administration 251
Remote Administration » HTTPS 255
Running Remote Administration under IIS 258
Template Manager » Web Services 587
Account Editor » Web Services 526

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.6.2.2 SSL & HTTPS



MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. SSL is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring Remote Administration to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » Remote Administration". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » Remote Administration".

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 487

This screen only applies to Remote Administration when using MDaemon's built-in web server. If you configure Remote Administration to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

Accept the Following Connection Types

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

HTTP only
Choose this option if you do not wish to allow any HTTPS connections to Remote Administration. Only HTTP connections will be accepted.

HTTP and HTTPS
Choose this option if you want to enable SSL support within Remote Administration, but do not wish to force your Remote Administration users to use HTTPS. Remote Administration will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the Remote Administration TCP port designated on the Web Server 252 screen.

HTTPS only
Choose this option if you wish to require HTTPS when connecting to Remote Administration. Remote Administration will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

HTTP redirected to HTTPS
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

HTTPS port
This is the TCP port that Remote Administration will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in Remote Administration's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the Remote Administration port that is designated on the Web Server 252 screen. If you are still allowing HTTP connections to Remote Administration then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

Select certificate to use for HTTPS/SSL

This box displays your SSL certificates. Click a certificate to designate it as the one Remote Administration will use. Double-click a certificate to open it in the Certificate dialog for review.

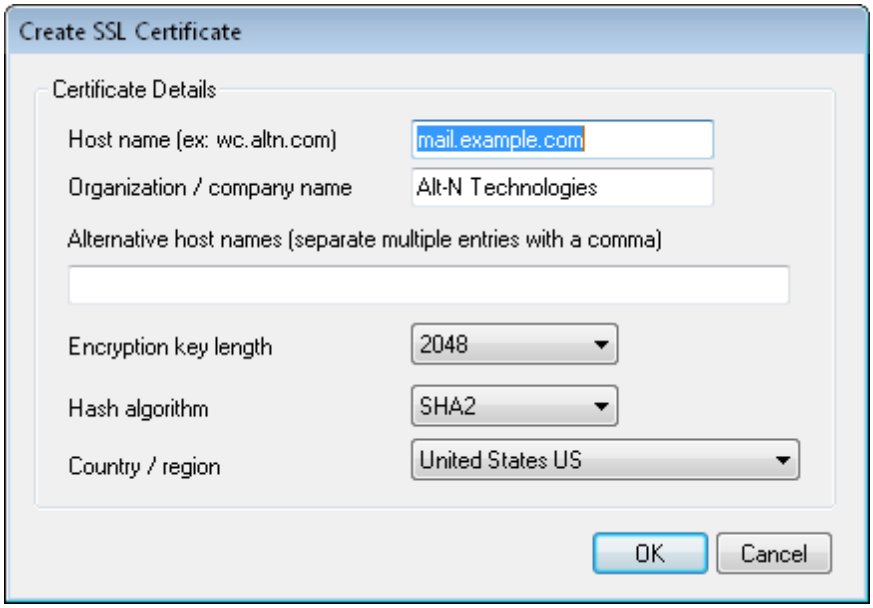
MDaemon does not support multiple certificates for Remote Administration. All domains must share a single certificate. If you have more than one domain then enter those domain names (and any others that you wish to use to access Remote Administration) into the option called "*Alternative host names (separate multiple entries with a comma)*" outlined below.

Delete
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Host name
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

Organization/company name
Enter the organization or company that "owns" the certificate here.

Alternative host names (separate multiple entries with a comma)
MDaemon does not support multiple certificates — all Remote Administration domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Country/region
Choose the country or region in which your server resides.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Restart web server

Click this button to restart the web server. The web server must be restarted before a new certificate will be used.

For more information on SSL and Certificates, see:

Running Remote Administration under IIS 258
SSL and Certificates 487
Creating and Using SSL Certificates 500

For more information on Remote Administration, see:

Remote Configuration 251
Remote Administration » Web Server 252
Web Access Defaults 587
Account Editor » Web 526

3.6.2.3 Running Remote Administration under IIS

MDaemon is equipped with a built-in web server, which means that Remote Administration doesn't require Internet Information Server (IIS) to operate. However, it does support IIS, and can therefore function as an ISAPI DLL.

To configure to operate under IIS 5:

1. Stop Remote Administration from running. You can do this by right-clicking on the Remote Administration entry under *Servers* in the left pane of the MDaemon GUI, and then clicking **Toggle Active/Inactive**.

2. Open the IIS management program (**Start→Settings→Control Panel→Administrative Tools→Internet Services Manager**).

3. Right-click **Default Website** and then select **New→Virtual Directory**.

4. Follow the Wizard as it takes you through the steps of creating a Virtual Directory. The following are suggested names and locations for data to be typed into the Wizard, but will vary depending on your installation of MDaemon and the location of MDaemon's Remote Administration component.

   a. Alias: "`WebAdmin`". Click **Next**.
   b. Directory: "`c:\mdaemon\webadmin\templates`". Click **Next**.
   c. Click **Next**.
   d. Click **Finish**.

5. Set the Execute Permissions to **Scripts Only**.

6. Set the Application Protection to **Low (IIS Process)**.

7. Click the **Configuration** button in the Application Settings section of the Virtual

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Directory tab.

8. On the **Mappings** tab click the **Add**.

9. In the **Executable** field enter "`c:\mdaemon\webadmin\templates\WebAdmin.dll`". Note: This field cannot contain any spaces. If the path contains a space it must be converted to 8.3 format. The `dir /x` command will show the 8.3 name for a file or directory.

10. In the **Extension** field enter "`.wdm`" and select the radio button for **All Verbs**.

11. Click the **Script Engine** box.

12. Click **OK**.

13. All other mappings can be removed if you choose, then click the **OK**.

14. On the **Documents** tab add `login.wdm` as a Default Document and remove all other entries from the list.

15. In MDaemon, go to **Setup→Web & IM Services→Remote Administration** and click **Remote Administration runs using external webserver**.

16. In **Remote Administration URL** type "`/WebAdmin/login.wdm`".

17. Click **OK**.

To configure to operate under IIS 6:

Create a new application pool for Remote Administration:

1. Stop Remote Administration from running. You can do this by right-clicking on the Remote Administration entry under *Servers* in the left pane of the MDaemon GUI, and then clicking **Toggle Active/Inactive**.

2. Open the IIS management program (**Start→Settings→Control Panel→Administrative Tools→Internet Services Manager**).

3. Right-click **Application Pools**.

4. Click **New→Application Pool**.

5. In the Application pool ID field type "`Alt-N`" and click **OK**.

6. Right-click **Alt-N**

7. Click **Properties**.

8. Click **Performance** tab.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

9. Clear "**Shutdown worker processes after being idle for**" and "**Limit the kernel request queue**".
10. Click **Identity** tab.
11. In the drop-down for Predefined, choose **Local System**.
12. Click **OK**.

Create a virtual directory for Remote Administration:

1. Open the IIS management program (**Start→Settings→Control Panel→Administrative Tools (Internet Services Manager)**).
2. Right-click your web site and then select New (Virtual Directory).
3. Specify an alias for the virtual directory (for example, "`WebAdmin`").
4. In the Path field, type the path to the Remote Administration Templates directory — for example, "`C:\Program Files\Alt-N Technologies\WebAdmin\Templates`".
5. Leave the **Read** and **Run Scripts** options checked.
6. Finish the wizard and right-click on the Virtual Directory that was created.
7. Select **Properties**.
8. On the Home Directory tab change the application pool to "Alt-N".
9. Click the Configuration button.
10. Click **Add** to add an ISAPI extension mapping.
11. In the Executable field enter the path to the `WebAdmin.dll` file. For example, "`C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll`".
12. In the Extension field enter "`.wdm`"
13. Click the boxes for **Script Engine** and **Verify the file exists**.
14. Click **OK**.
15. All other mappings can be removed if you choose, then click the **OK**.
16. Select the **Documents** tab.
17. Ensure that **Enable default content page** is checked.
18. Ensure that only "`login.wdm`" exists in the list.
19. Click the **Ok** and exit the virtual directory properties dialog.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Add `.WDM` to list of allowed web extensions:

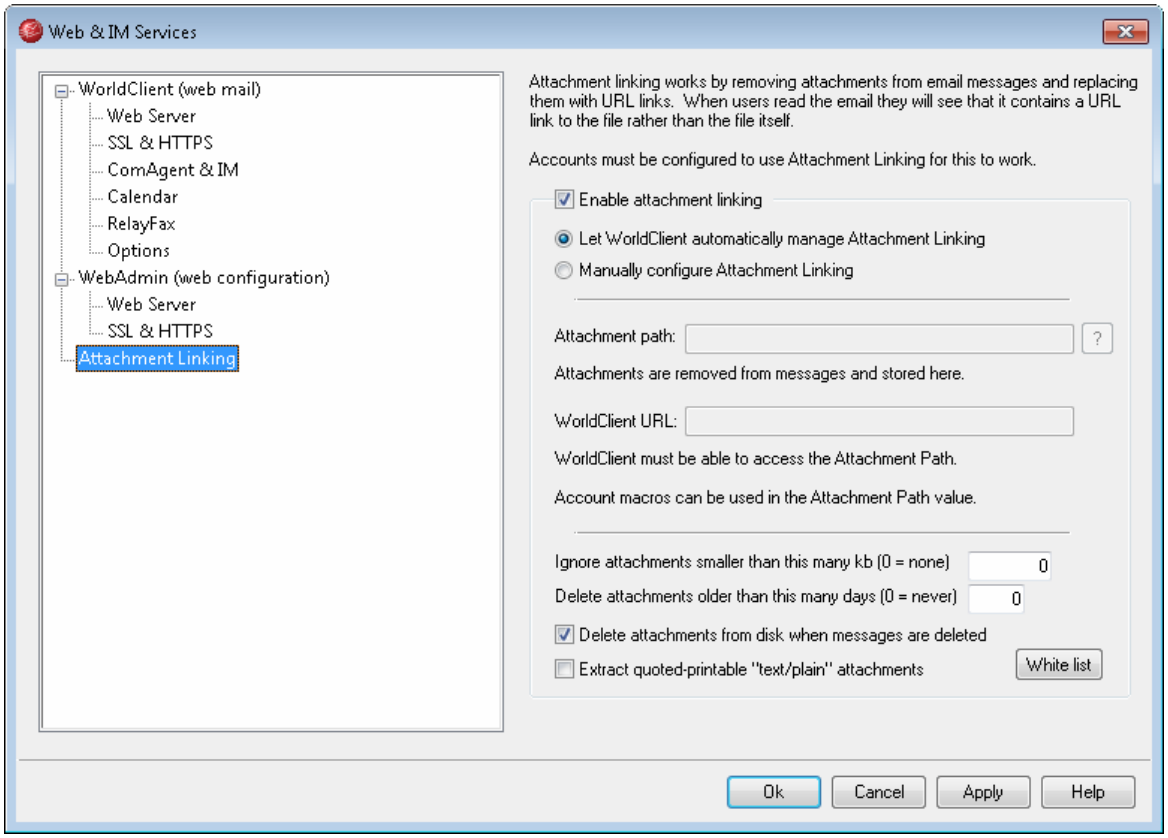
1. Click on the **Web Service Extensions** folder (in the IIS MMC).
2. Click **Add new web service extension**.
3. In the Extension name field enter "`WebAdmin`".
4. Click **Add** and then browse to the WebAdmin ISAPI extension. For example: `C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll`.
5. Check **Set extension status to allowed**.
6. Click **OK**.
7. In MDaemon, go to **Setup→Web & IM Services→Remote Administration** and click **Remote Administration runs using external web server**.
8. In **Remote Administration URL** type "`/WebAdmin/login.wdm`".
9. Click **OK**.

For more information on Remote Administration, see:

Remote Administration 251
Remote Administration » Web Server 252
Remote Administration » SSL & HTTPS 255
Template Manager » Web Services 587
Account Editor » Web Services 526

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.6.3 Attachment Linking


Web & IM Services
WorldClient (web mail)
Web Server
SSL & HTTPS
ComAgent & IM
Calendar
RelayFax
Options
WebAdmin (web configuration)
Web Server
SSL & HTTPS
Attachment Linking
Attachment linking works by removing attachments from email messages and replacing them with URL links. When users read the email they will see that it contains a URL link to the file rather than the file itself.
Accounts must be configured to use Attachment Linking for this to work.
Enable attachment linking
Let WorldClient automatically manage Attachment Linking
Manually configure Attachment Linking
Attachment path:
Attachments are removed from messages and stored here.
WorldClient URL:
WorldClient must be able to access the Attachment Path.
Account macros can be used in the Attachment Path value.
Ignore attachments smaller than this many kb (0 = none)
0
Delete attachments older than this many days (0 = never)
0
Delete attachments from disk when messages are deleted
Extract quoted-printable "text/plain" attachments
White list
Ok
Cancel
Apply
Help

Attachment Linking (`Setup » Web & IM Services » Attachment Linking`) is a feature that makes it possible for MDaemon to remove all attachments from incoming email messages, store them in a designated location, and then place URL links to the files in each message from which they are extracted. The recipients can then click those links to download the files. This can greatly speed up mail processing when your users retrieve their messages or synchronize their mail folders, since the messages will be devoid of large attachments. It can also provide increased security and an increased level of protection for your users, because attachments can be stored in a central location for monitoring by the administrator and will not be downloaded automatically to mail clients where they might be executed automatically. Further, if you choose the "*Let WorldClient automatically manage Attachment Linking*" option, management of the file locations and the WorldClient URL is handled automatically. If you choose to manage Attachment Linking manually, you can specify the location where the files will be stored, and you can use special macros to make the location dynamic. In order for Attachment Linking to work, it must be enabled globally using the option on this screen, and each Account that you wish to use it must be configured specifically to do so on the Attachments 539 screen of the Account Editor. On that same screen there is also an option for applying Attachment Linking to outbound messages as well; the account's outbound messages will have attachments extracted and replaced with a link to the stored files. Finally, the links to the attachments that MDaemon will place in messages do not contain direct file paths. Instead they contain a unique identifier (GUID) that the server uses to map the file to the actual path. This GUID map is stored in the `AttachmentLinking.dat` file.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Attachment Linking will try to use the file name provided in the MIME headers (if present). If the file name is longer than 50 characters then only the last 50 characters will be used. If the file name is missing an extension, ".att" will be appended.

By default, the Attachment Linking feature places the text, "MDaemon replaced the following files with these links:" into certain emails. If you wish to change that text, add the following key to your MDaemon.ini file, located in the \app\ folder, then restart MDaemon:

```
[AttachmentLinking]
HeaderText=This Is My Text.
```

Enable attachment linking
Click this checkbox to enable Attachment Linking for all accounts that are specifically configured to use it on the Attachments 539 screen of the Account Editor. When you enable this global option you will be asked if you also wish to enable the account specific option for all MDaemon accounts. If you choose "Yes" then Attachment Linking will be enabled for all accounts, and the corresponding option on the New Accounts 598 template will also be enabled. If you choose "No" then the Attachment Linking feature will be enabled but the account specific option will not—you must manually activate it for each account that you wish to use it. When Attachment Linking is enabled, the WorldClient server must remain active.

Let WorldClient automatically manage Attachment Linking
This is the default option when Attachment Linking is enabled. Use this option if you wish to let WorldClient handle Attachment Linking automatically. Extracted files will be stored at: "...\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\".

Manually configure Attachment Linking
Choose this option if you wish to designate the folder in which extracted file attachments will be stored. You must designate both the attachment path and the WorldClient URL when you choose this option.

Attachment path
Use this text box to designate the folder in which to store extracted file attachments. You can set a static file path or use template 583 and script 621 macros to make the path dynamic. For example, "$ROOTDIR$\Attachments\$DOMAIN$\" will group all attachments into a subfolder named for the domain to which the user belongs, which is under another subfolder called "Attachments" contained in MDaemon's root folder (usually C:\MDaemon\). So, for "user1@example.com" the above example would cause the extracted attachments to be placed in the subfolder, "C:\MDaemon\Attachments\example.com\." You could further subdivide attachment storage by appending the "$MAILBOX$" template macro to the above example. This would cause user1's files to be stored in a subfolder beneath "\example.com\" called "user1." Therefore the new file path would be: "C:\MDaemon\Attachments\example.com\user1\."

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

WorldClient URL
Enter WorldClient's URL here (e.g. "`http://mail.example.com:3000/WorldClient.dll`"). MDaemon will use this URL when inserting the links to extracted attachments in messages.

Ignore attachments smaller than this many KB (0 = none)
This is the minimum size required before an attachment will be extracted from a message. Use this option if you do not wish to extract smaller attachments. If set to "0" then Attachment Linking will extract all attachments, no matter how small.

Delete attachments older than this many days (0 = never)
Use this option if you wish to set a limit on the number of days that attachments will be stored. As part of the daily cleanup event MDaemon will remove any stored attachments that are older than the designated limit, if those attachments are contained within the default attachment folder or one of its subfolders. The default folder is: "`<MDaemonRoot>\Attachments\...`". Attachments will not be removed if you customize the attachment folder to point elsewhere. This option is disabled by default (set to "0").

Delete attachments from disk when messages are deleted
Click this option if you want to delete extracted attachments from the server whenever the messages to which they are linked are deleted.

When this option is enabled and a user collects his email via a POP3 client that is not configured to leave messages on the server, then all of his extracted attachments will be irretrievably lost. If this option is not enabled then no attachments will be lost, but a great deal of your hard drive space could eventually be taken up by outdated and useless files that their original recipient no longer wants or needs. Virtually all POP clients have the ability to leave messages on the server.

Extract quoted printable “text/plain” attachments
By default, quoted printable `text/plain` attachments will not be extracted. Click this checkbox if you wish to include them in automatic extraction.

White List
Click this button to open the Attachment Linking white list. Include any file names that you do not wish to extract from messages. `Winmail.dat` is included on this list by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

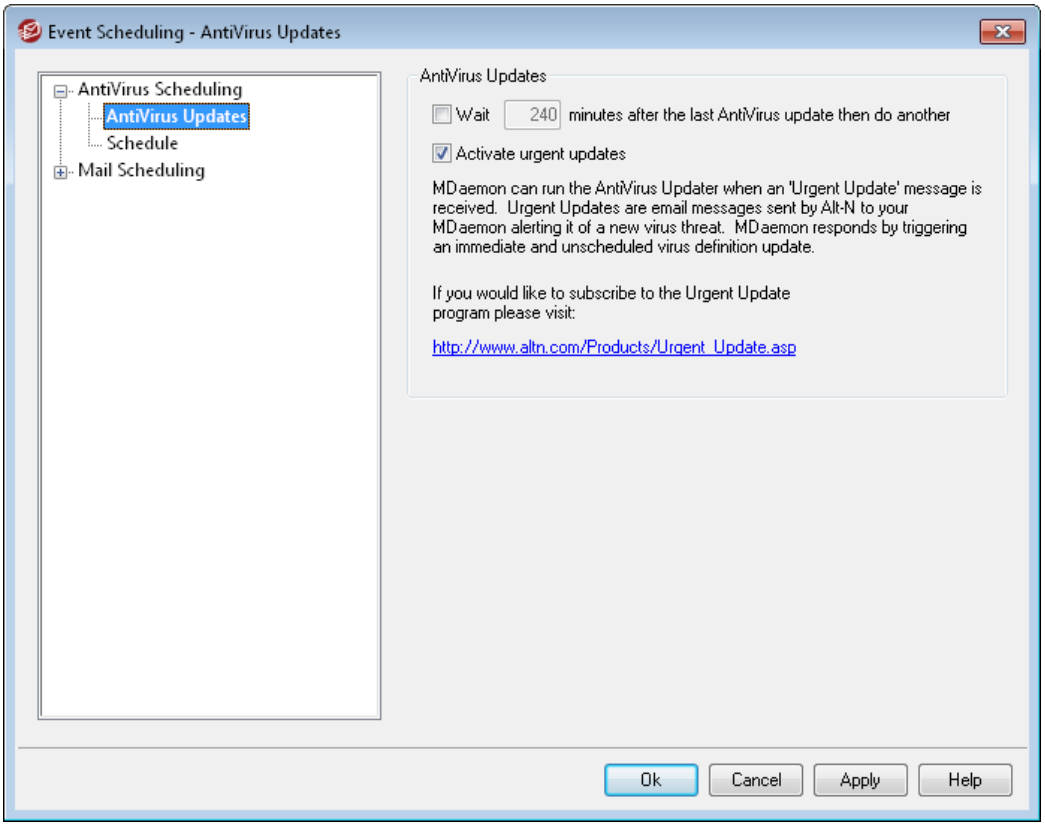
See:

New Accounts Template 582
Account Editor » Attachments 539
Template Macros 583
Script Macros 621

3.7 Event Scheduling

3.7.1 AntiVirus Scheduling

3.7.1.1 AntiVirus Updates


Event Scheduling - AntiVirus Updates
AntiVirus Scheduling
AntiVirus Updates
Schedule
Mail Scheduling
AntiVirus Updates
Wait
240
minutes after the last AntiVirus update then do another
Activate urgent updates
MDaemon can run the AntiVirus Updater when an 'Urgent Update' message is received. Urgent Updates are email messages sent by Alt-N to your MDaemon alerting it of a new virus threat. MDaemon responds by triggering an immediate and unscheduled virus definition update.
If you would like to subscribe to the Urgent Update program please visit:
http://www.altn.com/Products/Urgent_Update.asp
Ok
Cancel
Apply
Help

AntiVirus Updates

Wait XX minutes after the last AntiVirus update then do another
Click this checkbox and specify the number of minutes that you want SecurityPlus for MDaemon to wait before checking for new virus signature updates. Note, this is actually the number of minutes that SecurityPlus for MDaemon will *attempt* to wait after the last time you checked for an update, whether the update was triggered by the scheduler or manually. The scheduler and manually triggered updates are given precedence over this setting and will therefore reset this counter if a SecurityPlus update event is triggered by one of those other methods. Thus, for example, if you

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

have this option set to check for updates every 240 minutes and you manually check for an update after 100 minutes, this counter will be reset to 240.

Urgent Updates

Activate urgent updates
Click this checkbox to activate the urgent updates feature. With this feature enabled, SecurityPlus for MDaemon will immediately connect to the update location and download the high-priority update whenever MDaemon receives an "Urgent Update" message. To receive these messages you must add your domain to the Urgent Updates system at altn.com.

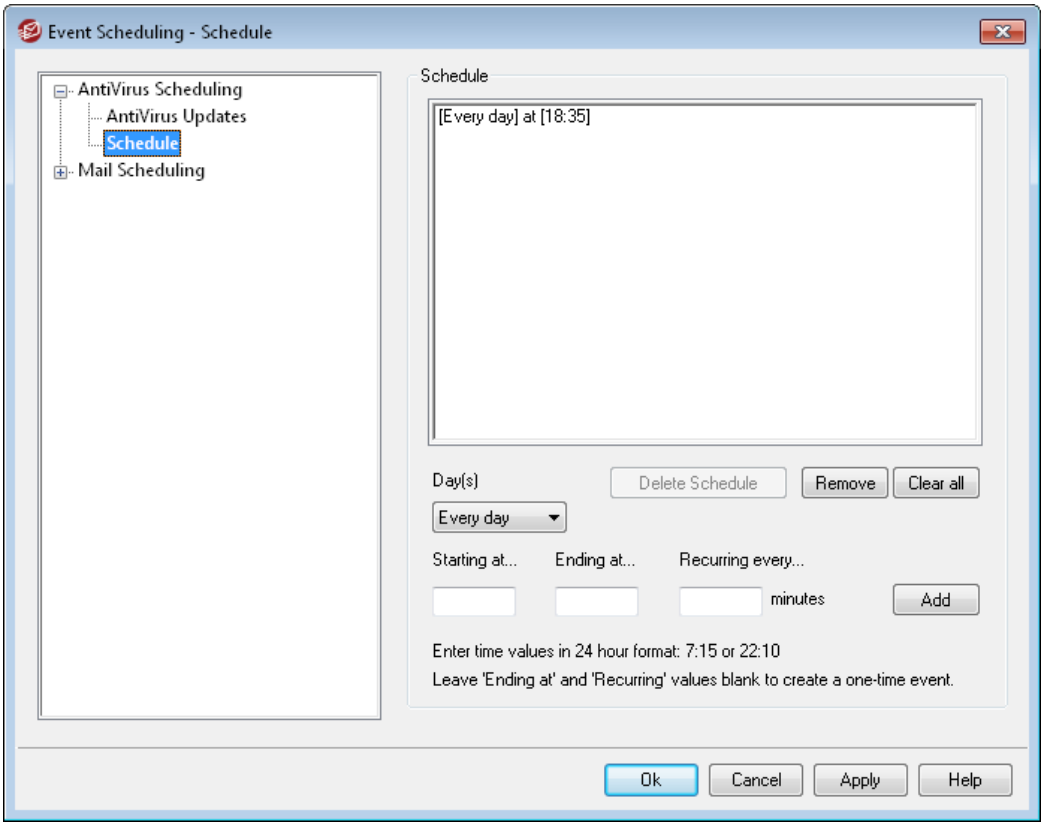
You must have the "*Verify...DKIM signatures*" option on the DKIM Verification 447 screen enabled to use this feature.

See:

AntiVirus Update Schedule 267
AntiVirus 383
AntiVirus Updater 386

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.7.1.2 Schedule



Use the AntiVirus Update Schedule to designate specific times for SecurityPlus 362 to check for AntiVirus updates. The schedule is located at: Setup » Event Scheduling » AntiVirus Updates » Schedule.

Schedule

Remove
To remove an event from the list, select the entry and then click this button.

Clear all
This button removes all entries from the schedule.

Creating Schedule Events

Day(s)
When creating a new event for the schedule, first select the day or days on which this scheduled update check event will occur. You can select: every day, weekdays (Monday thru Friday), weekends (Saturday and Sunday), or specific days of the week.

Starting at...
Enter the time that you wish the update check to start. The time value must be in 24 hour format, from 00:00 to 23:59. If you wish this to be a single event rather than recurring event, this is the only time value that you will enter (leave the *Ending*

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

at... and *Recurring every...* options blank).

Ending at...
Enter the time that you wish the update check event to end. The time value must be in 24 hour format, from 00:01 to 23:59, and it must be greater than the *Starting at...* value. For example, if the *Starting at...* value were "10:00" then this value could be from "10:01" to "23:59". Leave this option blank if you wish it to be a single event rather than recurring event.

Recurring every [xx] minutes
This is the time interval at which SecurityPlus will check for updates between the designated *Starting at...* and *Ending at...* times. Leave this option blank if you wish it to be a single event rather than recurring event.

Add
Once you have designated the *Day(s)* and *Starting at...* time, and the optional *Ending at...* time and *Recurring every...* value, click this button to add the event to the schedule.

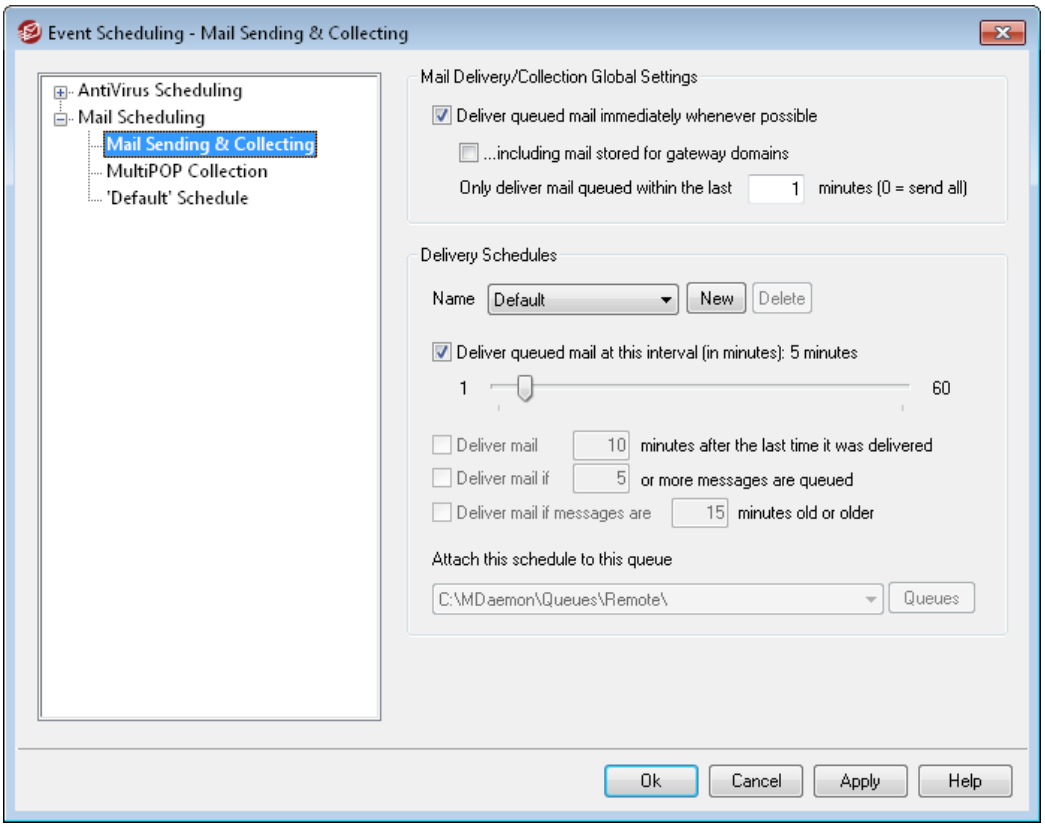
See:

AntiVirus Updates 383
AntiVirus 383
AntiVirus Updater 386

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.7.2 Mail Scheduling

3.7.2.1 Mail Sending & Collecting


Event Scheduling - Mail Sending & Collecting
AntiVirus Scheduling
Mail Scheduling
Mail Sending & Collecting
MultiPOP Collection
'Default' Schedule
Mail Delivery/Collection Global Settings
Deliver queued mail immediately whenever possible
...including mail stored for gateway domains
Only deliver mail queued within the last 1 minutes (0 = send all)
Delivery Schedules
Name Default New Delete
Deliver queued mail at this interval (in minutes): 5 minutes
1 60
Deliver mail 10 minutes after the last time it was delivered
Deliver mail if 5 or more messages are queued
Deliver mail if messages are 15 minutes old or older
Attach this schedule to this queue
C:\MDaemon\Queues\Remote\ Queues
Ok Cancel Apply Help

Click Setup » Event Scheduling to open MDaemon's Event Scheduler. Using this screen you can schedule MDaemon's Remote mail processing events as extensively or as simply as you prefer. You can use a counter to process mail at regular intervals, or you can schedule exact times for mail delivery and collection using the Mail Schedule 273 screens. You can also set conditions that will trigger mail processing at unscheduled times such as when a certain number of messages are waiting to be delivered, or when a message has been waiting a specified amount of time. Further, you can create custom schedules that you can assign to custom remote mail queues. Custom schedules make it possible for you to set different schedules for different types of messages. For example, you could create schedules for large messages, mailing list messages, certain domains, and so on.

If you have installed SecurityPlus for MDaemon 362, use the AntiVirus Updates 265 section of the Event Scheduler to schedule how often MDaemon will check for AntiVirus updates.

Mail Delivery/Collection Global Settings

Deliver queued mail immediately whenever possible
When this option is enabled and a message arrives and is queued for remote delivery, rather than waiting for the next scheduled processing interval or some

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

other event to trigger mail processing, MDaemon will immediately process and deliver all remote mail that has been queued within the number of minutes designated in the *Only deliver mail queued within the last [xx] minutes* option below.

...including mail stored for gateway domains
Click this check box if you also want messages for Domain Gateways to be delivered immediately. However, this only applies to gateways with the *Deliver stored messages each time MDaemon processes remote mail* option enabled on the Gateway 168 screen of the Gateway Editor.

Only deliver mail queued within the last [xx] minutes (0=send all)
This option governs how recently messages must have been queued before the *Deliver queued mail immediately whenever possible* option above will spool them for delivery. When that option triggers remote mail processing, instead of attempting to deliver everything in the queue, MDaemon will process only those messages that were queued within the designated number of minutes. The entire queue will still be processed, however, when the *Process...queue* toolbar button is pressed or when any other normal scheduling event triggers remote mail processing. By default, this option is set to one minute. You can set it to "0" if you wish to process the entire queue every time remote mail processing is triggered, but that is not recommended since it is much less efficient.

The above options only apply to the Default schedule. They are unavailable for custom schedules (see the *Name...* option below).

Name...
Use this drop-down list box to select a schedule to edit. The Default schedule will always be used for the regular, remote mail queue and for DomainPOP and MultiPOP collected mail. For configurations using dialup services, the Default schedule will also be used for LAN Domains, which are remote domains that you have designated as residing on your local area network and therefore do not require RAS dialup. Other schedules can be assigned to custom remote mail queues, and messages can be routed to those custom queues 658 automatically by using the Content Filter 364. When you are finished editing a schedule's options, click OK or select another schedule for editing. If you make changes to a schedule and then select another schedule, a confirmation box will open asking you whether you wish to save or discard the currently selected schedule's changes before switching to the other schedule.

New
Click this option to create a new schedule. A box will open so that you can designate a name for it. After the schedule's name is designated, a corresponding Mail Schedule 273 screen will be created for it in the menu on the left. Use that screen to assign times to that schedule.

Delete
To delete a custom schedule, first select it in the *Name...* drop-down list and then click *Delete*. A confirmation box will open asking you if you are sure you wish to delete it. Deleting a custom schedule will not delete any custom remote queue or

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

content filter rules associated with it. However, if you delete a custom queue then any schedules associated with that queue will also be deleted, and all associated content filter rules as well.

Deliver queued mail at this interval (in minutes)
Click the check box and slide this bar left or right to specify the time interval between mail processing sessions. It can be configured to count down from a range of 1 to 60 minutes. After that amount of time, MDaemon will process remote mail before beginning the countdown again. When this check box is cleared, *Remote Mail* processing intervals will be determined by the other scheduling options.

Deliver mail [xx] minutes after the last time it was delivered
Use this option when you want a remote mail processing session to occur at a regular time interval after the last session occurred, regardless of the trigger that initiated the session. Unlike the rigidly fixed intervals used when setting up specific times or when using the *Deliver queued mail at this interval* slide bar, this option's time interval will reset each time mail is processed.

Deliver mail if [xx] or more messages are queued
When this option is enabled, MDaemon will trigger a mail session whenever the number of messages waiting in the remote queue meets or exceeds the number that you specify here. These mail sessions are in addition to any other normally scheduled sessions.

Deliver mail if messages are [xx] minutes old or older
When this box is checked, MDaemon will trigger a mail session whenever a message has been waiting in the queue for the number of minutes specified. These sessions are in addition to any other normally scheduled sessions.

Queues

Attach this schedule to this queue
Use this option to associate the selected schedule with a specific custom remote mail queue. You can then use the content filter to create rules that will place certain messages in that queue. For example, if wanted to schedule mailing list messages destined for remote addresses to be delivered at some specific time, then you could create a custom queue for those messages, create a rule to put all of them into your custom queue, and then create a custom schedule and assign it to that queue.

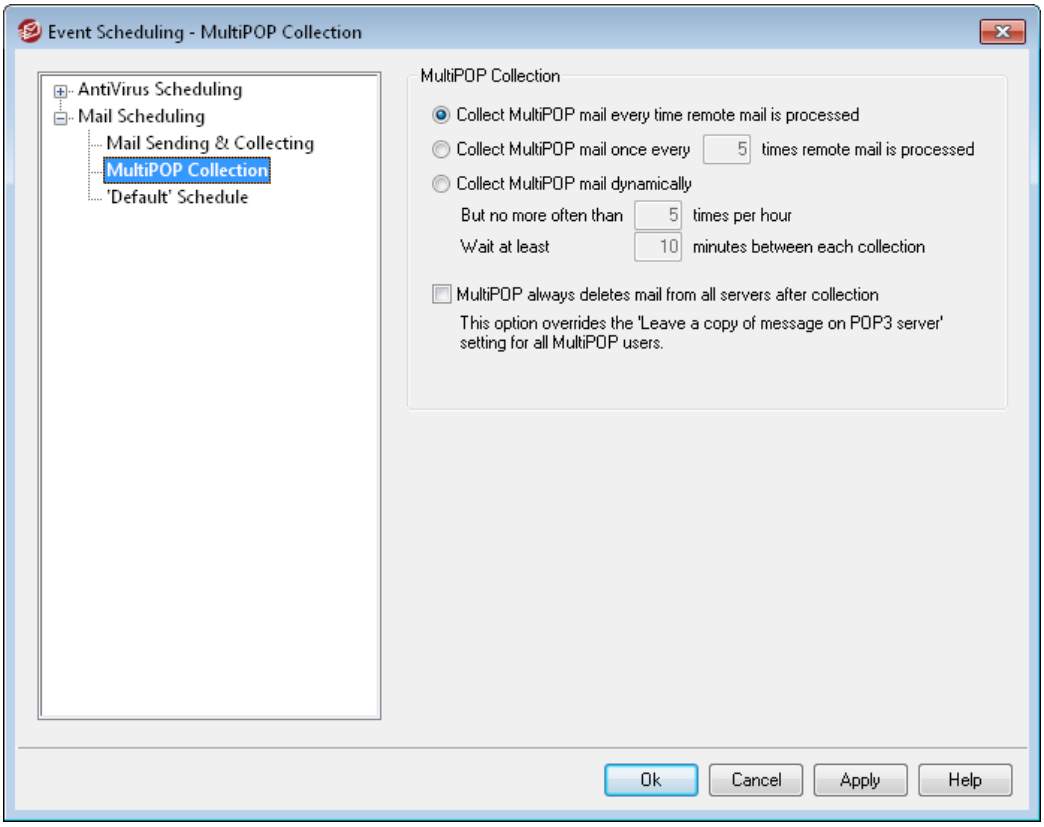
Queues
Click the button to open the Custom Queues 658 screen, on which you can create custom remote queues to use with the Event Scheduler.

See:

Mail Schedule 273
AntiVirus Updates 265

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.7.2.2 MultiPOP Collection


Event Scheduling - MultiPOP Collection
AntiVirus Scheduling
Mail Scheduling
Mail Sending & Collecting
MultiPOP Collection
'Default' Schedule
MultiPOP Collection
Collect MultiPOP mail every time remote mail is processed
Collect MultiPOP mail once every 5 times remote mail is processed
Collect MultiPOP mail dynamically
But no more often than 5 times per hour
Wait at least 10 minutes between each collection
MultiPOP always deletes mail from all servers after collection
This option overrides the 'Leave a copy of message on POP3 server' setting for all MultiPOP users.
Ok
Cancel
Apply
Help

MultiPOP Collection

Collect MultiPOP mail every time remote mail is processed
Choose this option if you want MDaemon to collect all MultiPOP 544 mail every time that remote mail is processed.

Collect MultiPOP mail once every XX times remote mail is processed
Choose this option and specify a numeral in the box if you want MultiPOP mail to be collected less often than remote mail is processed. The numeral denotes how many times remote mail will be processed before MultiPOP mail will be collected.

Collect MultiPOP mail dynamically
Choose this option if you wish to collect MultiPOP messages dynamically. Ordinarily, MultiPOP is collected for all users at the same time at each remote mail processing interval, or at every *x* number of intervals. When collected dynamically, MultiPOP messages are collected for each individual user when that user checks his or her local mail via POP, IMAP, or WorldClient rather than for all users at once. However, because MultiPOP collection is triggered by a user checking his email, any new MultiPOP messages collected will not be visible to the user until he checks his mail *again*. Thus, he would need to check his mail twice in order to see new MultiPOP messages. The first time to trigger MultiPOP and a second time to see the mail that was collected.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

But no more often than XX times per hour
In order to reduce the load that extensive use of MultiPOP can potentially place on your MDaemon, you can use this control to specify a maximum number of times per hour that MultiPOP can be collected for each user.

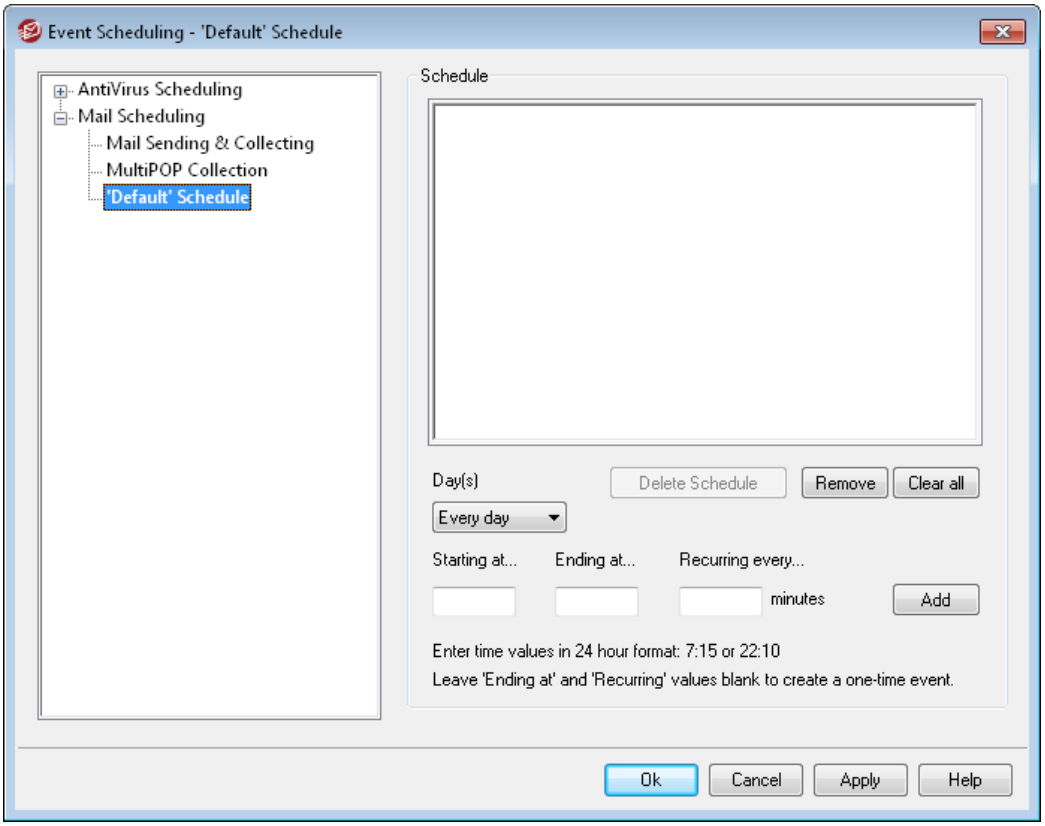
Wait at least XX minutes between each collection
This option can help to reduce the load on the mail server by limiting how frequently MultiPOP messages can be collected by each user. It will restrict MultiPOP mail collection to once every so many minutes per user. Specify the number of minutes that you wish to require the user to wait before being allowed to check MultiPOP again.

MultiPOP always deletes mail from all servers after collection
Click this check box if you wish to override the *Leave a copy of message on POP server* option (located on the MultiPOP 544 screen of the Account Editor) for all users. All messages will be deleted from each MultiPOP server after they are collected.

See:

MultiPOP 544

3.7.2.3 Mail Schedule



Each Mail Schedule corresponds to the schedule of the same name listed in the *Name*

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

drop-down list on the Mail Sending & Collecting 269 screen. Use each Mail Schedule to designate the specific times that remote mail processing will occur for that schedule. Mail Schedules are located at: Setup » Event Scheduling » Mail Scheduling » 'ScheduleName' Schedule.

Schedule

Delete Schedule
This button will delete the custom Mail Schedule. The schedule will be deleted and its entry will be removed from the *Name* drop-down list on the Mail Sending & Collecting 269 screen. After you click this button, a confirmation box will open asking if you are sure you want to delete the schedule. This option is only available for custom schedules — the Default Schedule cannot be deleted.

Remove
To remove an entry from the list, select the entry and then click this button.

Clear all
This button removes all entries from the schedule.

Creating Schedule Events

Day(s)
When creating a new event for the schedule, first select the day or days on which this scheduling event will occur. You can select: every day, weekdays (Monday thru Friday), weekends (Saturday and Sunday), or specific days of the week.

Starting at...
Enter the time that you wish the event to start. The time value must be in 24 hour format, from 00:00 to 23:59. If you wish this to be a single event rather than recurring event, this is the only time value that you will enter (leave the *Ending at...* and *Recurring every...* options blank).

Ending at...
Enter the time that you wish the event to end. The time value must be in 24 hour format, from 00:01 to 23:59, and it must be greater than the *Starting at...* value. For example, if the *Starting at...* value were "10:00" then this value could be from "10:01" to "23:59". Leave this option blank if you wish it to be a single event rather than recurring event.

Recurring every [xx] minutes
This is the time interval at which mail will be processed between the designated *Starting at...* and *Ending at...* times. Leave this option blank if you wish it to be a single event rather than recurring event.

Add
Once you have designated the *Day(s)* and *Starting at...* time, and the optional *Ending at...* time and *Recurring every...* value, click this button to add the event to the schedule.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Depending on your needs, it may be sufficient to use the simple scheduling options on the Mail Sending & Collecting 269 screen to control mail processing intervals. For example, it is pointless to make a specific schedule with events for every minute of every day when you can simply set the slider bar on Mail Sending & Collecting to one minute intervals and accomplish the same thing. On the other hand, if you want the processing intervals to be more than an hour apart, or only on certain days, then you can use some combination of the scheduling options and mail specific times.

See:

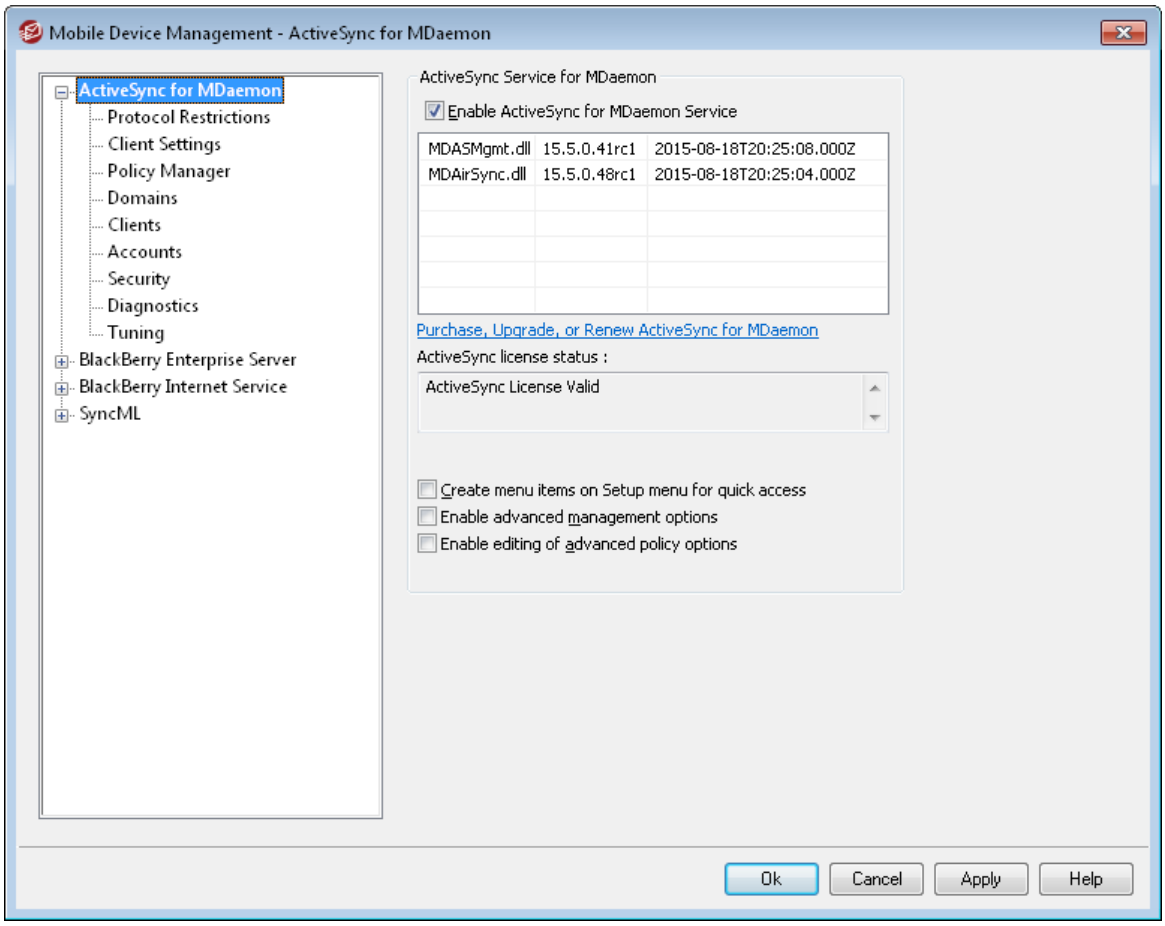
Mail Sending & Collecting 269
AntiVirus Updates 265
AntiSpam Updates 420

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.8 Mobile Device Management

3.8.1 ActiveSync for MDaemon

3.8.1.1 ActiveSync for MDaemon



MDaemon includes support for "ActiveSync for MDaemon," which is a separately licensed over-the-air (OTA) ActiveSync server. This server is capable of synchronizing a user's Email and PIM data (i.e. Contacts, Calendars, and Tasks) between his MDaemon/WorldClient account and an ActiveSync capable device. MDaemon's ActiveSync options are located under: `Setup » Mobile Device Management... » ActiveSync`. There are also user-specific options located on the Account Editor's ActiveSync for MDaemon 557 screens.

If you enable ActiveSync for MDaemon the first time using a trial key, it will operate for 30 days. After that, if you wish to continue using it you can acquire a license key from www.altn.com or your local distributor/reseller.

ActiveSync is a web-service extension that only works on ports **80** (for http) and **443** (for https). This is an ActiveSync implementation requirement. If ActiveSync is enabled and you are using WorldClient's built-in web server, but it is not running on port 80 or 443, then it will automatically begin running on port 80 in addition to whatever other ports you have configured on the Web Server 229 and SSL & HTTPS 234 screens. If you

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

are using another server for WorldClient such as IIS then you must manually configure it to use port 80 or 443.

If you intend to run ActiveSync under IIS you must call the ActiveSync DLL (`MDAirSync.dll`) when "`/Microsoft-Server-ActiveSync`" is requested. This is the request that all the ActiveSync clients will use. Some versions of IIS do not have this capability without downloading, installing, and configuring third party software.

All first time syncs with ActiveSync are a one way sync from the server to the device. You will lose related data on the device when you sync with ActiveSync for the first time. This is an ActiveSync implementation requirement. You should therefore backup your device data before using ActiveSync for the first time. Most devices that support ActiveSync warn the user that "**device data will be lost**," but some do not.

Enabling/Disabling ActiveSync

Click *Enable ActiveSync for MDaemon Service* to turn on ActiveSync for MDaemon. Then you can use the Domains 292 options to control whether or not it is available to all or some of your domains.

Advanced Interface Options

Create menu items on Setup menu for quick access
Check this box if you wish to add several ActiveSync-related menu items to the Setup menu on the toolbar, for quicker access to the ActiveSync configuration screens. This is disabled by default.

Enable advanced management options
By default the Diagnostics 310 and Tuning 312 screens are hidden from the navigation pane on the left side of the Mobile Device Managements dialog. These screens contain options governing various ActiveSync system settings and diagnostics tools, and in most cases they will rarely need to be accessed or adjusted by anyone. Enable this option if you want them to be visible.

Enable editing of advanced policy options
Enable this option if you want the Advance Settings tab to be visible on the ActiveSync Policy Editor 285. It contains various advanced policy settings that in most cases will not need to be changed. This option is disabled by default.

ActiveSync Autodiscover Service

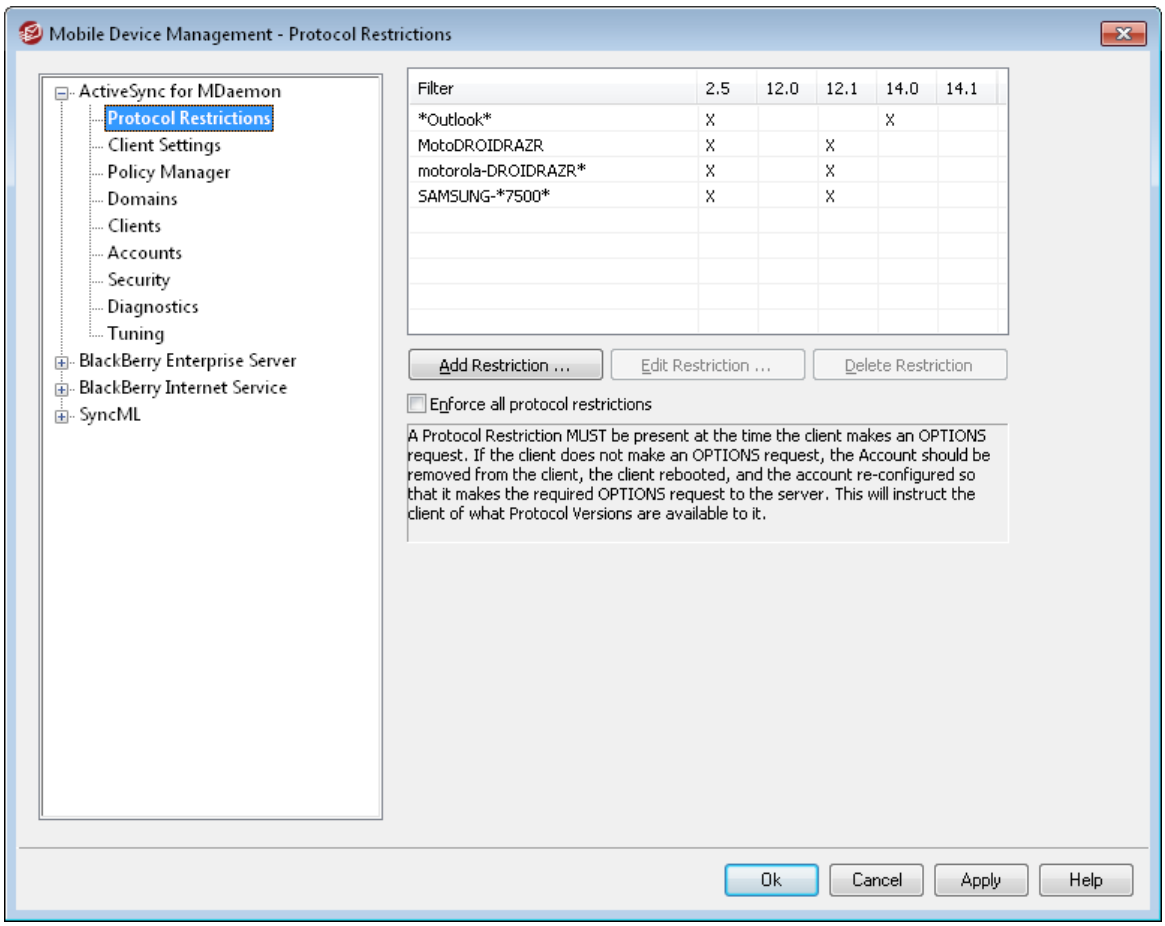
MDaemon supports the ActiveSync Autodiscover Service, which allows users to set up an ActiveSync account with just their email address and password, without needing to know the host name of the ActiveSync server. Autodiscover requires HTTPS 234 to be enabled, and for most systems it also requires that a new CNAME or A-record be added to DNS. "`autodiscover.<your-MDaemon-server>.com`" should resolve to the MDaemon server running ActiveSync (for example, `autodiscover.example.com`).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Account Editor » ActiveSync for MDaemon 557
SSL & HTTPS 234
Web Server 229

3.8.1.2 Protocol Restrictions



Device Protocol Restrictions

Use the options located under "Mobile Device Management... » ActiveSync » Protocol Restrictions" to tell certain clients and devices that they are restricted to specific ActiveSync protocols. This is useful when, for example, a certain type of device is found to have unreliable support for one protocol but reliable support for another. Using the Add/Edit Protocol Restriction 279 dialog, you can define restrictions based on User Agent or Device Type, and restrict the devices to any of the following ActiveSync protocol versions: 2.5, 12.0, 12.1, 14.0, and 14.1.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

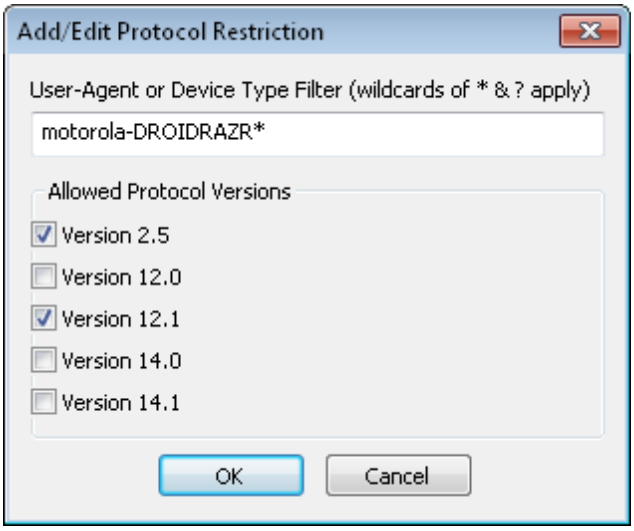
By default, protocol restrictions do not prevent a client from attempting to use a different protocol; they tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. If you wish to deny connections that attempt to use restricted protocols, use the *Enforce all protocol restrictions* option below.

Add Restriction
Click this button to open the Add/Edit Protocol Restriction dialog, used for adding your protocol restrictions.

Edit Restriction
To edit a protocol restriction, select an entry from the list and then click **Edit Restriction**. After making your desired changes in the restriction editor, click **OK**.

Delete Restriction
To delete a protocol restriction entry, select an entry from the list and then click **Delete Restriction**. Click **Yes** to confirm your decision to delete the restriction.

Add/Edit Protocol Restriction



User-Agent or Device Type Filter
Enter the User Agent or Device Type to which the restriction will apply. When identifying the agent, MDaemon uses up to and including the first "/" character in the string, if one is present. If not, then the entire string is used. If you do not know the exact name of the User Agent or Device Type, once the client has connected to MDaemon ActiveSync (MDAS) you can go to the Clients 297 screen, select the client from the list, and click Details. You can also find this info by examining the MDAS log file directly.

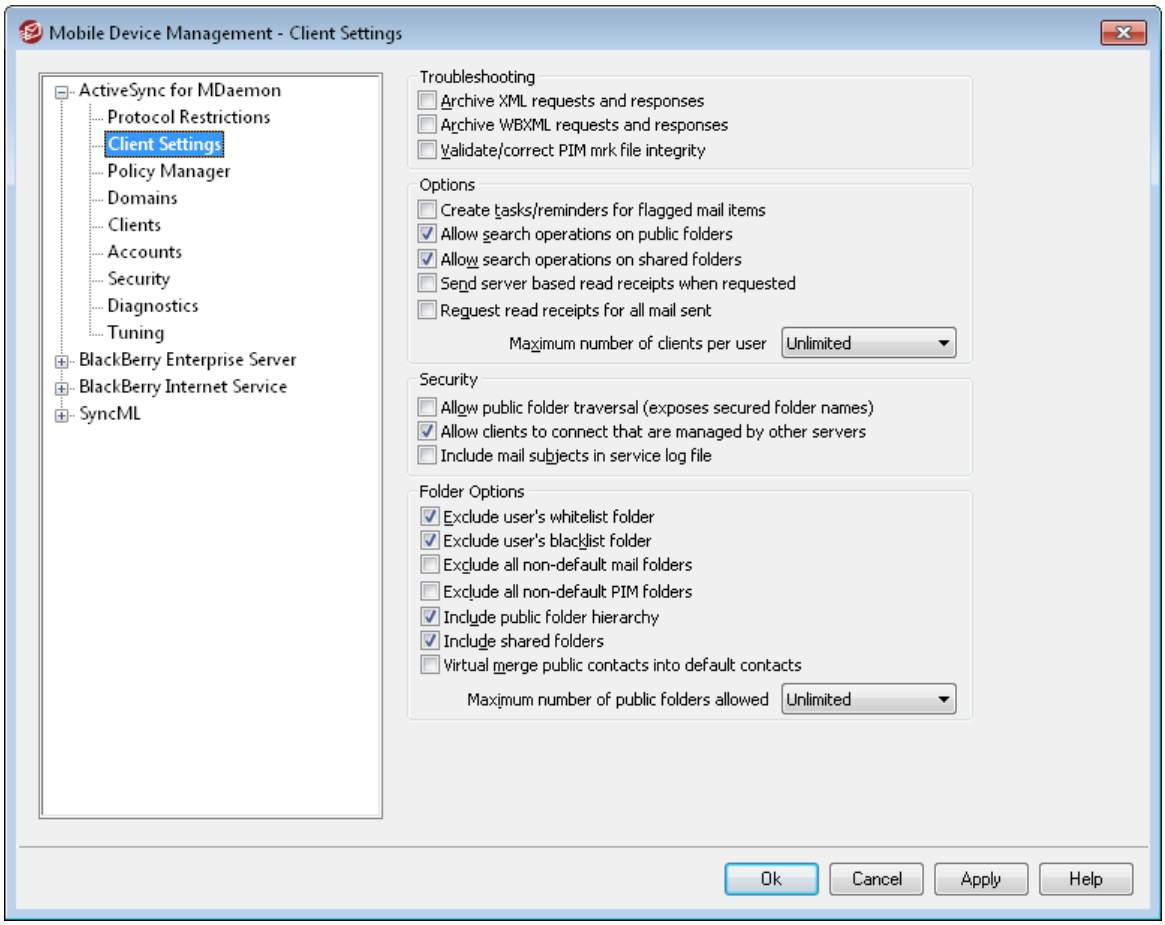
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Allowed Protocol Versions
Click each protocol that you wish to support for the device or agent. When the specified client connects to MDaemon it will be told to use only the protocols that you have selected.

Enforce all protocol restrictions

Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection.

3.8.1.3 Client Settings



This screen contains the global settings for managing ActiveSync clients. There are corresponding client settings under Mobile Device Management's Domains 292, Accounts 303, and Clients 297 screens for setting these options per domain, per account, and per client respectively. The global settings are set to specific values, but the domain, account, and client settings are by default set to *Inherit* their settings from their respective parent options. Therefore changing any setting on this screen will effectively change the same setting on all child screens, allowing you by default to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

manage all clients on the server by changing only the settings on this one screen. Conversely, changing a setting on a child screen will override its parent setting, allowing you to alter the settings at the domain, account, or client level if necessary.

Similar to Policies 284, which are assigned to the device and generally govern what the device can do, Client Settings govern what the server will do with regards to various client-related options, such as: governing how many separate ActiveSync clients an account can use, whether or not Public Folders will be synced to a device along with the account's personal folders, whether or not to include the user's whitelist folder, and so on.

Troubleshooting

Archive [XML | WBXML] requests and responses
Use the *Archive XML...* and *Archive WBXML...* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Options

Create Tasks/Reminders for flagged mail items
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email. This is disabled by default.

Allow search operations on Public Folders
Allows the client to search the Public Folders 218 to which it has access. This is allowed by default.

Allow search operations on Shared Folders
Allows the client to search the Shared Folders 547 to which it has access. This is allowed by default.

Send server based read receipts when requested.
Enable this option if you want the server to support read confirmation requests an issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Request read receipts for all mail sent
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Maximum number of clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Security

Allow Public Folder traversal (exposes secured folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 220 for both the subfolder (i.e. child folder) and all parent public folders 218 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Allow clients to connect that are managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Disable this option if you do not wish to allows those clients to connect.

Include mail subjects in service log file
Enable this option if you wish to include each message's Subject header in the ActiveSync log file. This is not recommended, and this option is disabled by default.

Folder Options

Exclude user's [whitelist/blacklist] folder
By default the user's whitelist and blacklist contact folders are not synced with devices. They are generally only used by MDaemon, to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Exclude all non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Exclude all non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include Public Folder hierarchy
Check this box if you want the public folders 218 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Include shared folders
Check this box if you want the shared folders 87 to which a user has access to be

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

included in the user's folder list on ActiveSync devices. This is enabled by default.

Virtual merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Maximum number of Public Folders allowed
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Preview Effective Settings

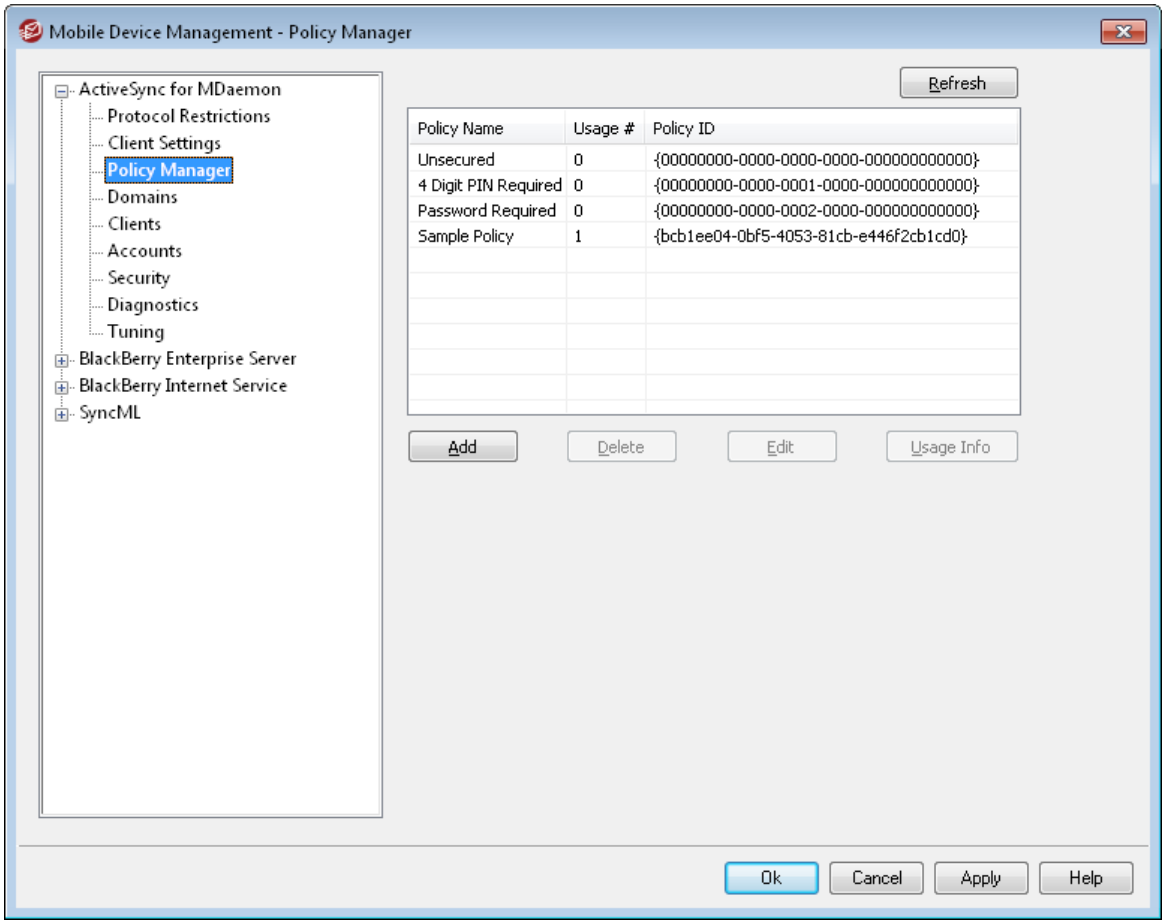
This button is available on all of the child Client Settings screens (i.e. domains 292, accounts 303, and clients 297). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Domains 292
ActiveSync » Accounts 303
ActiveSync » Clients 297

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.8.1.4 Policy Manager



Use this screen to manage the ActiveSync Policies that can be assigned to user devices to govern various options. Predefined policies are provided, and you can create, edit and delete your own. Default policies can be assigned per domain 292 and per per account 303, and policies can be assigned to specific clients 297.

Not all ActiveSync devices recognize or apply policies consistently. Some may ignore policies or certain policy elements altogether, and others may require a device reboot before changes take effect. Further, when attempting to assign a new policy to a device, it will not be applied to the device until the next time it connects on its own to the ActiveSync server; policies cannot be "pushed" to devices until they connect.

ActiveSync Policies

Add
Click this button to open the ActiveSync Policy Editor, used for creating and editing your policies.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Delete
To delete a policy, select a custom policy from the list and then click **Delete**. Click **Yes** to confirm the action. The predefined policies cannot be deleted.

Edit Policy
To edit a policy, select a custom policy from the list and then click **Edit**. After making your desired changes in the policy editor, click **OK**. The predefined policies cannot be edited.

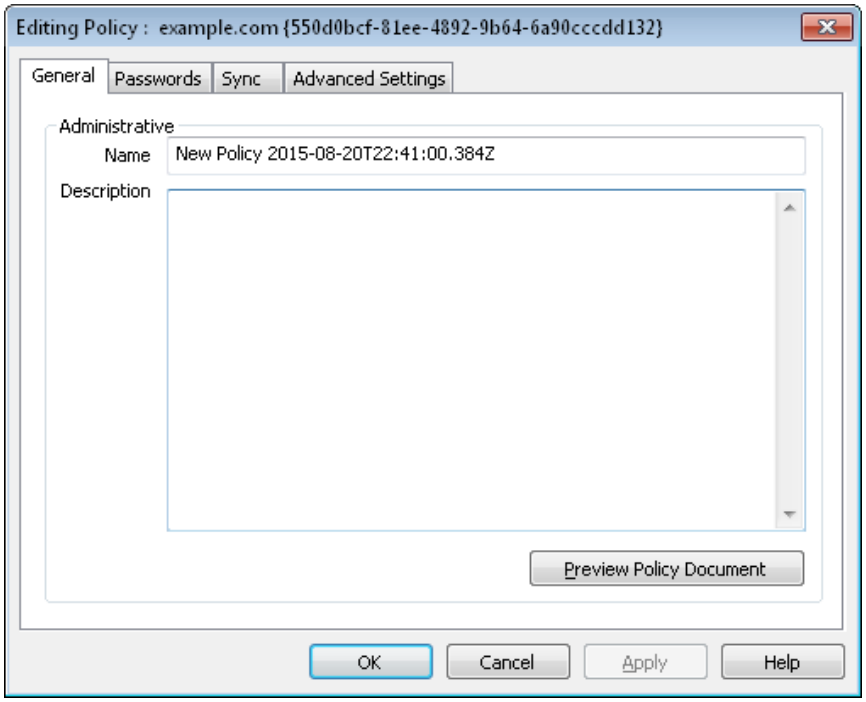
Usage Info
Select a policy and then click this button to view a list of all domains, accounts, and clients that are set to use this policy.

ActiveSync Policy Editor

The ActiveSync Policy Editor has four tabs: General, Passwords, Sync, and Advanced Settings. The Advanced Settings tab is hidden unless you activate *Enable editing of advanced policy options* 276, located on the ActiveSync for MDaemon screen.

General

Use this screen to designate a name and description for your policy. You can also preview the XML policy document.



Administrative

Name
Specify a name for your custom policy here.

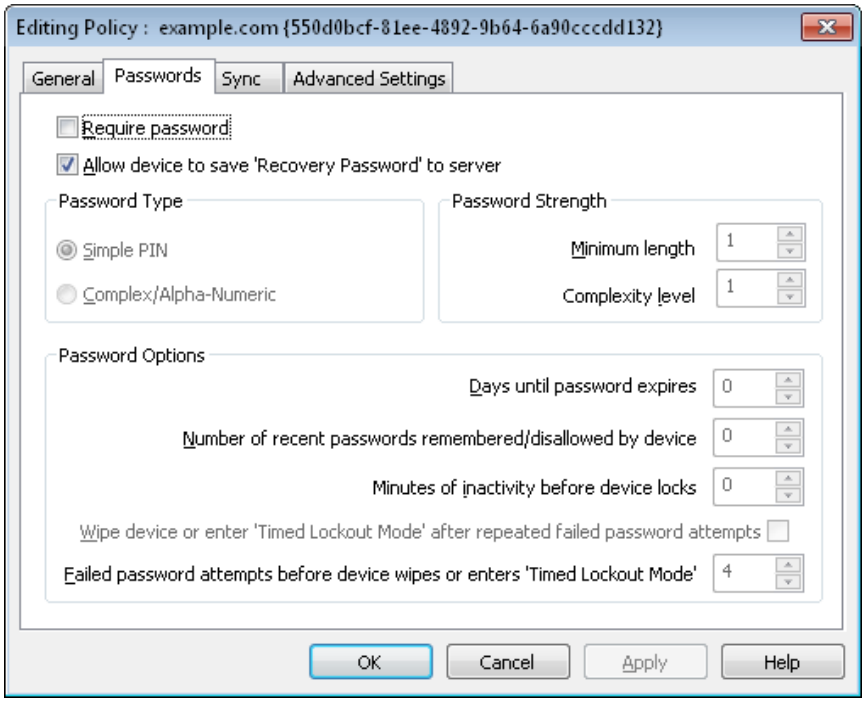
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Description
Use this area to describe your custom policy. This description appears on the Apply Policy dialog when selecting a policy to apply to a domain, account, or client.

Preview Policy Document
Click this button to preview the XML policy document for this policy.

Passwords

Password options and requirements for the policy are designated on this tab.



Require password
Check this box if you wish to require a password on the device. It is disabled by default.

Allow device to save 'Recovery Password' to server
Enable this option if you wish to allow clients to use ActiveSync's Recovery Password option, which allows a device to save a temporary recovery password to the server to unlock the device if the password is forgotten. The administrator can find this recover password under the client's Details 297. Most devices do not support this feature.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Password Type

Simple PIN
How this option is implemented is largely dependent on the device, but selecting *Simple PIN* as the password type generally means that no restrictions or complexity requirements are placed on the device password, other than the *Minimum password length* option below. This allows simple passwords such as: "111," "aaa," "1234," "ABCD" and the like.

Complex/Alpha-Numeric
Use this policy option if you wish to require more complex and secure device passwords than the *Simple PIN* option. Use the *Complexity level* option below to define exactly how complex the password must be. This is the default selection when a password is required by the policy.

Password Strength

Minimum length
Use this option to set the minimum number of characters that the device password must contain, from 1-16. This option is set to "1" by default.

Complexity level
Use this option to set the complexity level requirement for *Complex/Alpha-numeric* device passwords. The level is the number of different types of characters that the password must contain: uppercase letters, lowercase letters, numbers, and non-alphanumeric characters (such as punctuation or special characters). You can require from 1-4 character types. For example, if this option were set to "2", then the password must contain at least two of the four character types: uppercase and numbers, uppercase and lowercase, numbers and symbols, and so on. This option is set to "1" by default.

Password Options

Days until password expires (0=never)
This is the number of days allowed before the device's password must be changed. This option is disabled by default (set to "0").

Number of recent passwords remembered/disallowed by device (0=none)
Use this option if you wish to prevent the device from reusing a specified number of old passwords. For example, if this option is set to "2" and you change your device password, you will not be able to change it to either of the last two passwords that were used. The option is disabled by default (set to "0").

Minutes of inactivity before device locks (0=never)
This is the number of minutes that a device can go without any user input before it will lock itself. This password option is disabled by default (set to "0").

Wipe device or enter 'Timed Lockout Mode' after repeated failed password attempts
When this option is enabled and the user fails the designated number of

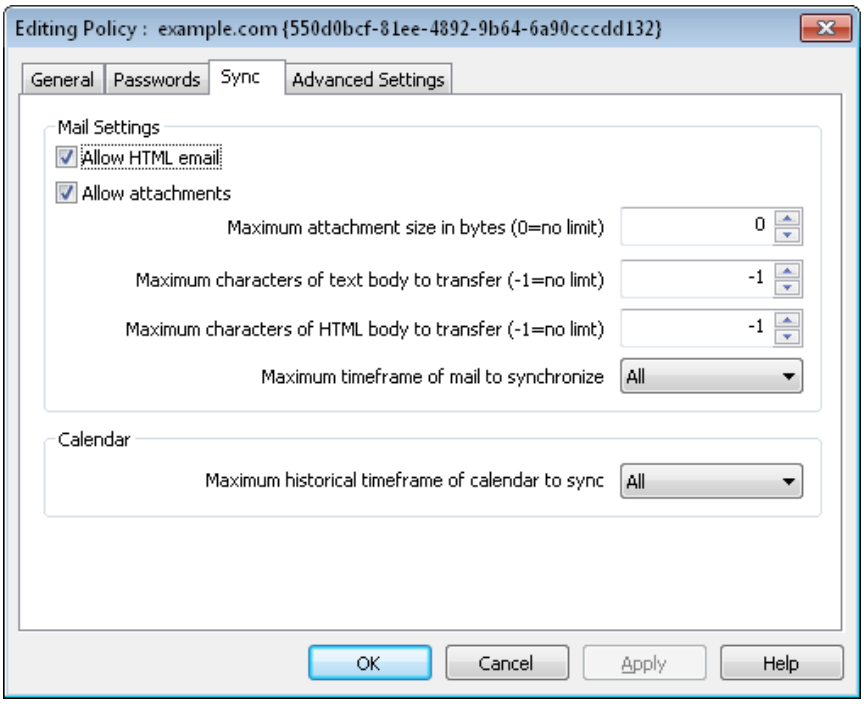
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

password attempts, the device will either lock itself for a certain amount of time or perform a wipe of all data, depending on the device. This option is disabled by default.

Failed password attempts before device wipes or enters 'Timed Lockout Mode'
When the "*Wipe device..*" option above is enabled and a user fails this many password attempts, the device will be wiped or the 'Timed Lockout Mode' will be triggered, depending on the device.

Sync

This screen contains various settings governing HTML email, allowing attachments, limiting the number of characters to transfer, and the maximum mail and calendar timeframes to sync.



Mail Settings

Allow HTML email
By default HTML-formatted email can be synced/sent to ActiveSync clients. Uncheck this box if you wish to send only plain text.

Allow attachments
Allows the device to download file attachments. This option is enabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Max attachment size in bytes (0=no limit)
This is the maximum size of attachment that can be automatically downloaded to the device. There is no size limit set for this option by default (set to "0").

Maximum characters of text body to transfer (-1=no limit)
This is the maximum number of characters in the body of plain text-formatted emails that will be sent to the client. If the message body contains more characters than are allowed, the body will be truncated to the specified limit. By default there is no limit set (option set to "-1"). If you set the option to "0" then only the message header is sent.

Maximum characters of HTML body to transfer (-1=no limit
This is the maximum number of characters in the body of HTML-formatted emails that will be sent to the client. If the message body contains more characters than are allowed, the body will be truncated to the specified limit. By default there is no limit set (option set to "-1"). If you set the option to "0" then only the message header is sent.

Maximum timeframe of mail to synchronize
This is the amount of past email, by date range from today, that can be synchronized by the device. By default this is set to "All," meaning that all email can be synchronized no matter how old it is.

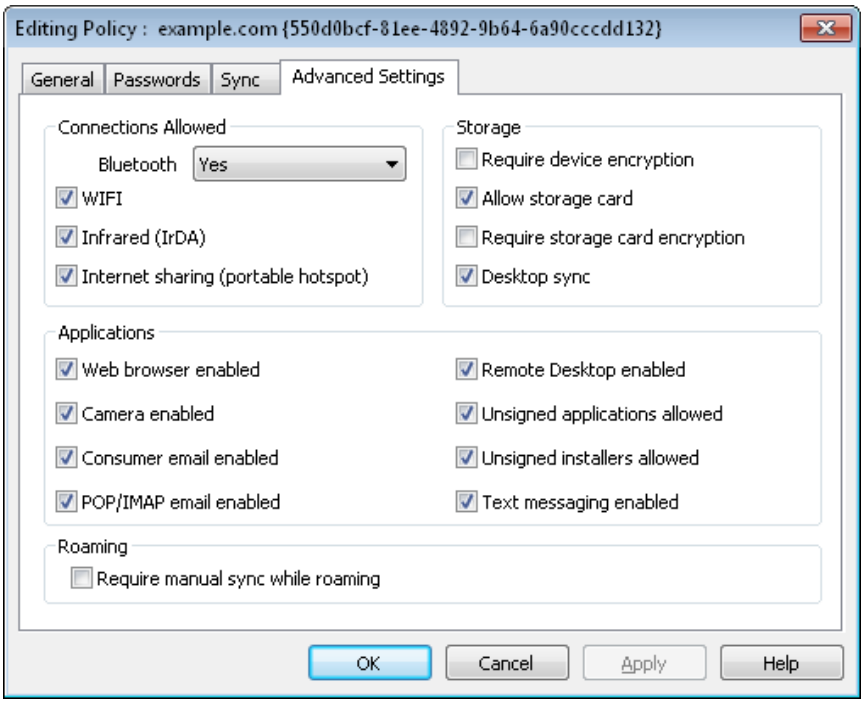
Calendar

Maximum historical timeframe of calendar to sync
This is how far back from today that past calendar entries can be synchronized by the device. By default this is set to "All," meaning that all past entries can be synchronized no matter how old they are.

Advanced Settings

The Advanced Settings tab contains options governing the types of connections allowed, whether certain applications can be enabled, storage and encryption, and roaming.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



This tab is hidden unless you activate *Enable editing of advanced policy options*[276], located on the ActiveSync for MDaemon screen.

Connections Allowed

Bluetooth
Use this option to designate whether or not Bluetooth connections are allowed on the device. You can choose **Yes** to allow Bluetooth connections, **No** to prevent them, or **Handsfree** to restrict Bluetooth to Handsfree only. This option is set to **Yes** by default.

WIFI
Allows WIFI connections. Enabled by default.

Infrared (IrDA)
Allows Infrared (IrDA) connections. Enabled by default.

Internet sharing (portable hotspot)
This option allows the device to use Internet sharing (portable hotspot). It is enabled by default.

Storage

Require device encryption
Click this option if you wish to require encryption on the device. Not all devices will enforce encryption. This is disabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Allow storage card
Allows a storage card to be used in the device. This is enabled by default.

Require storage card encryption
Use this option if you wish to require encryption on a storage card. This is disabled by default.

Desktop sync
Allows Desktop ActiveSync on the device. Enabled by default.

Applications

Web browser enabled
Allows the use of a browser on the device. This option is not supported on some devices, and it may not apply to 3rd party browsers. It is enabled by default.

Camera enabled
Allows the use of a camera on the device. This option is enabled by default.

Consumer email enabled
Device allows the user to configure a personal email account. When disabled, the types of email accounts or services that are prohibited is entirely dependent on the particular ActiveSync client. This option is enabled by default.

POP/IMAP email enabled
Allows access to POP or IMAP email. Enabled by default.

Remote Desktop enabled
Allows the client to use Remote Desktop. Enabled by default.

Unsigned applications allowed
This option allows unsigned applications to be used on the device. This is enabled by default.

Unsigned installers allowed
This option allows unsigned installers to be run on the device. This is enabled by default.

Text messaging enabled
This option allows text messaging on the device. Text messaging is enabled by default.

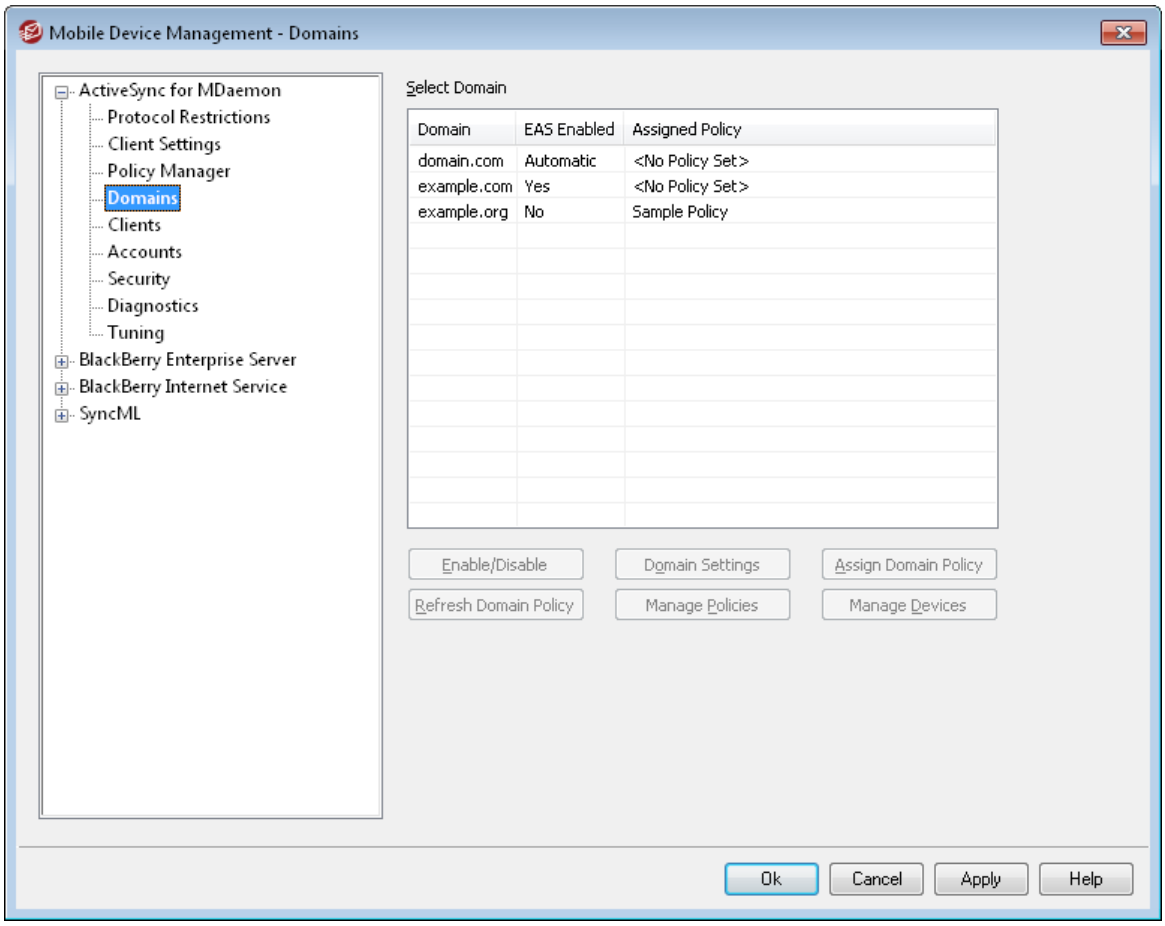
Roaming

Require manual sync while roaming
Use this policy option if you wish to require the device to synchronize manually while roaming. Allowing automatic synchronization while roaming

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

could increase data costs for the device, depending on its carrier and data plan. This option is disabled by default.

3.8.1.5 Domains



Use this screen to manage the ActiveSync settings for your domains 121. You can enable or disable ActiveSync for each domain, assign a default ActiveSync policy 284, manage the default client settings, and manage devices associated with the domain.

Enabling/Disabling ActiveSync for Specific Domains

To set the ActiveSync state for a specific domain:

1. Click a domain in the list.
2. Click **Enable/Disable** until the EAS Enabled column shows the desired state. Choose **Yes** to enable ActiveSync, **No** to disable it, or **Automatic** if you want the domain to use the default setting.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

In order to use ActiveSync you will need to properly configure an ActiveSync client on the user's device. For instructions on how to do this, follow the *Purchase, Upgrade, or Review ActiveSync for MDaemon* link on the ActiveSync for MDaemon 276 screen and scroll down to the device setup instructions.

Setting the Default ActiveSync State

Domains with the *EAS Enabled* column set to **Automatic** will take their ActiveSync setting from a key in the MDaemon.ini file. By default this key is set to "Yes." To change the default ActiveSync state for domains:

1. Open `\MDaemon\app\MDaemon.ini` in a text editor such as Notepad.
2. Under `[ActiveSync]`, set `EnableActiveSyncDomainDefault=Yes` to enable ActiveSync for domains by default, or change it to "`=No`" to disable it for them.
3. Save the file.

Domain Settings

Select a domain and click this button to manage the Client Settings for the domain. By default these settings are inherited from the global Client Settings 280 screen. See Managing a Domain's Client Settings 293 below.

Assigning a Default ActiveSync Policy

To assign a default ActiveSync policy to a domain:

1. Select a domain from the list.
2. Click **Assign Domain Policy**. This opens the Apply Policy dialog.
3. Click the Assigned Policy drop-down list and choose the desired policy.
4. Click **OK**.

Refresh Domain Policy

Click this button to refresh the time stamp of the assigned domain policy. They will cause any devices that use that policy to provision.

Manage Policies

Click this button to manage your ActiveSync Policies 284.

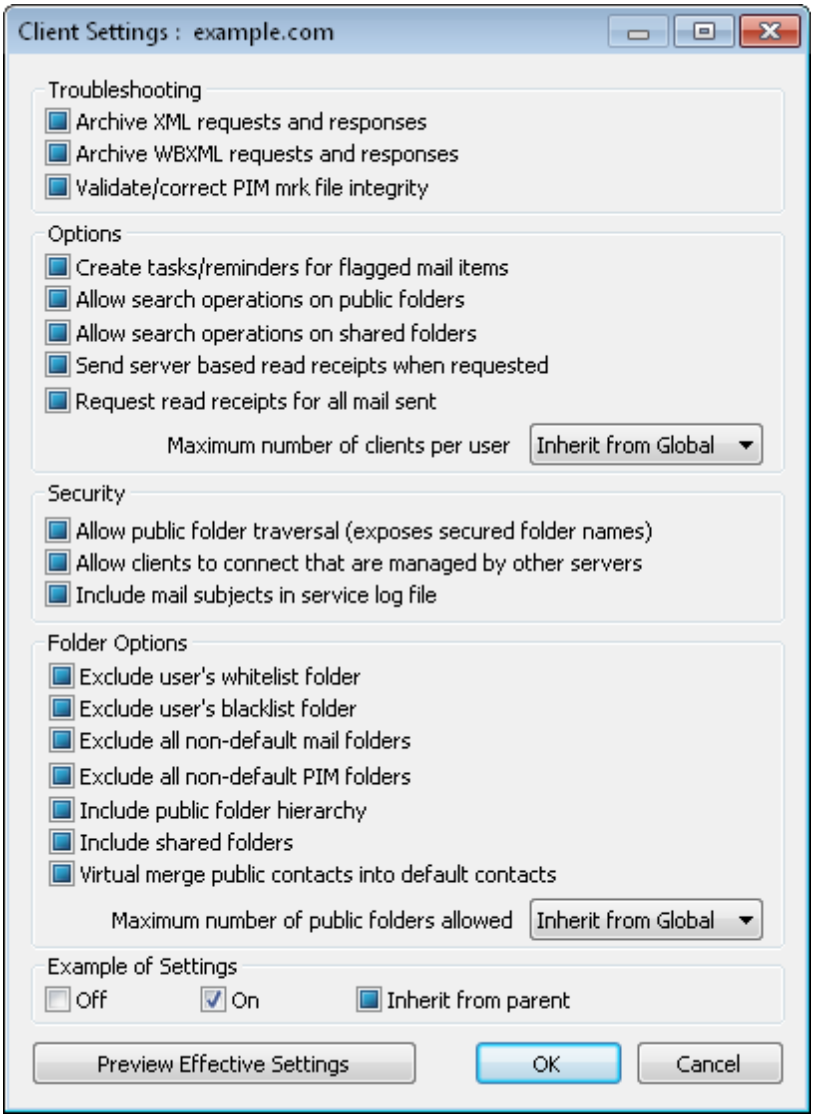
Manage Devices

Select a domain and click this button to manage the devices 297 associated with that domain.

Managing a Domain's Client Settings

The Domain Settings screen allows you to manage the default settings for accounts and clients associated with the domain.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.


Client Settings : example.com
Troubleshooting
Archive XML requests and responses
Archive WBXML requests and responses
Validate/correct PIM mrk file integrity
Options
Create tasks/reminders for flagged mail items
Allow search operations on public folders
Allow search operations on shared folders
Send server based read receipts when requested
Request read receipts for all mail sent
Maximum number of clients per user
Inherit from Global
Security
Allow public folder traversal (exposes secured folder names)
Allow clients to connect that are managed by other servers
Include mail subjects in service log file
Folder Options
Exclude user's whitelist folder
Exclude user's blacklist folder
Exclude all non-default mail folders
Exclude all non-default PIM folders
Include public folder hierarchy
Include shared folders
Virtual merge public contacts into default contacts
Maximum number of public folders allowed
Inherit from Global
Example of Settings
Off
On
Inherit from parent
Preview Effective Settings
OK
Cancel

By default all of the options on this screen are set to "Inherit from parent," which means that each option will take its setting from the corresponding option on the global Client Settings 280 screen. Similarly, the client settings screens for this domain's Accounts 303 will inherit their settings from this screen, since the Domain Settings screen is their parent screen. Any changes made to the options on this screen will be reflected on those screens. Below that, individual clients 297 also have settings screens that inherit their settings from the account-level settings. This configuration makes it possible for you to make changes to all of a domain's accounts and clients simply by making changes to this one screen, while also making it possible for you to override those settings for any account or client as needed.

Troubleshooting

Archive [XML | WBXML] requests and responses
Use the *Archive XML...* and *Archive WBXML...* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Options

Create Tasks/Reminders for flagged mail items
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email. This is disabled by default.

Allow search operations on Public Folders
Allows the client to search the Public Folders 218 to which it has access. This is allowed by default.

Allow search operations on Shared Folders
Allows the client to search the Shared Folders 547 to which it has access. This is allowed by default.

Send server based read receipts when requested.
Enable this option if you want the server to support read confirmation requests an issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Request read receipts for all mail sent
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Maximum number of clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default.

Security

Allow Public Folder traversal (exposes secured folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 220 for both the subfolder (i.e. child folder) and all parent public folders 218 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Allow clients to connect that are managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

conflict with the other ActiveSync server's policy. Disable this option if you do not wish to allows those clients to connect.

Include mail subjects in service log file
Enable this option if you wish to include each message's Subject header in the ActiveSync log file. This is not recommended, and this option is disabled by default.

Folder Options

Exclude user's [whitelist/blacklist] folder
By default the user's whitelist and blacklist contact folders are not synced with devices. They are generally only used by MDaemon, to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Exclude all non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Exclude all non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include Public Folder hierarchy
Check this box if you want the public folders 218 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Include shared folders
Check this box if you want the shared folders 87 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Virtual merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Maximum number of Public Folders allowed
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

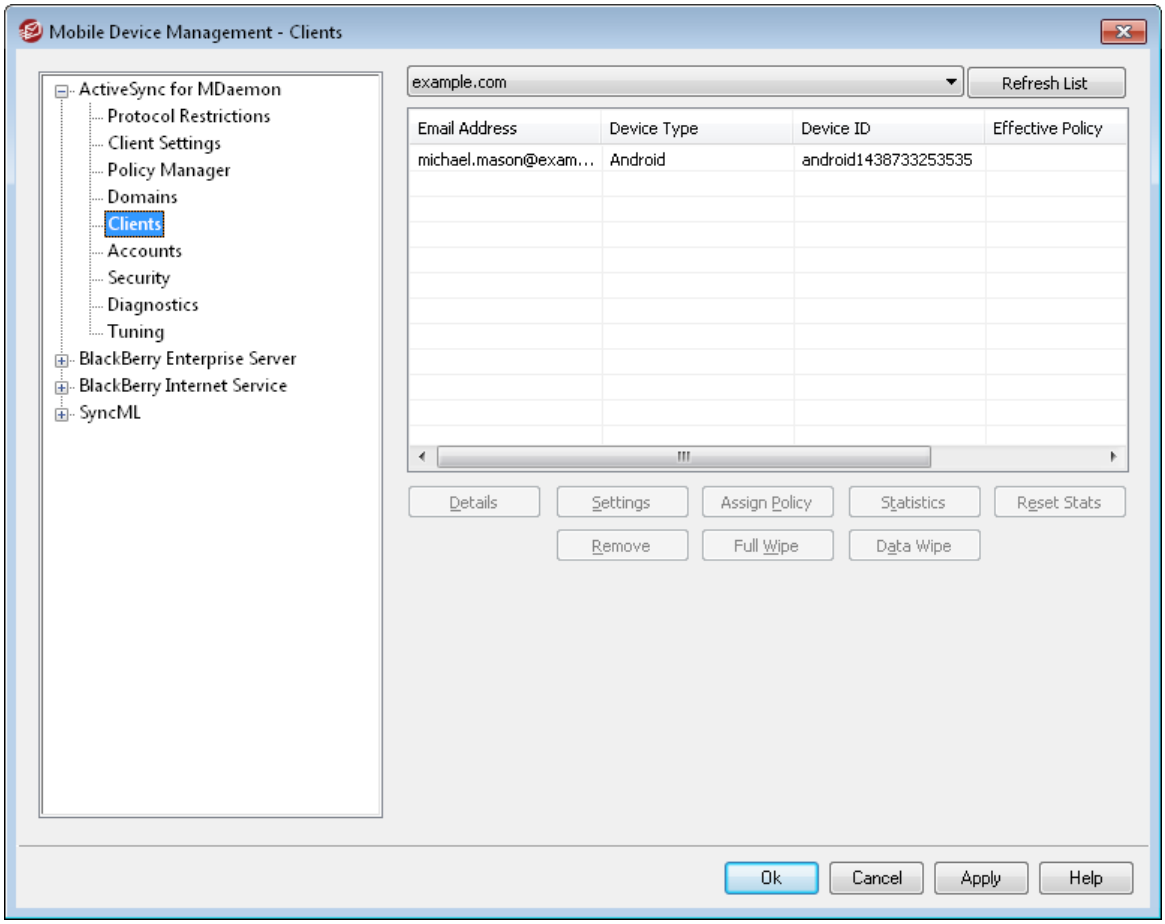
Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 292, accounts 303, and clients 297). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

Domain Manager » ActiveSync Client Settings 143
ActiveSync » Policy Manager 284
ActiveSync » Clients 297

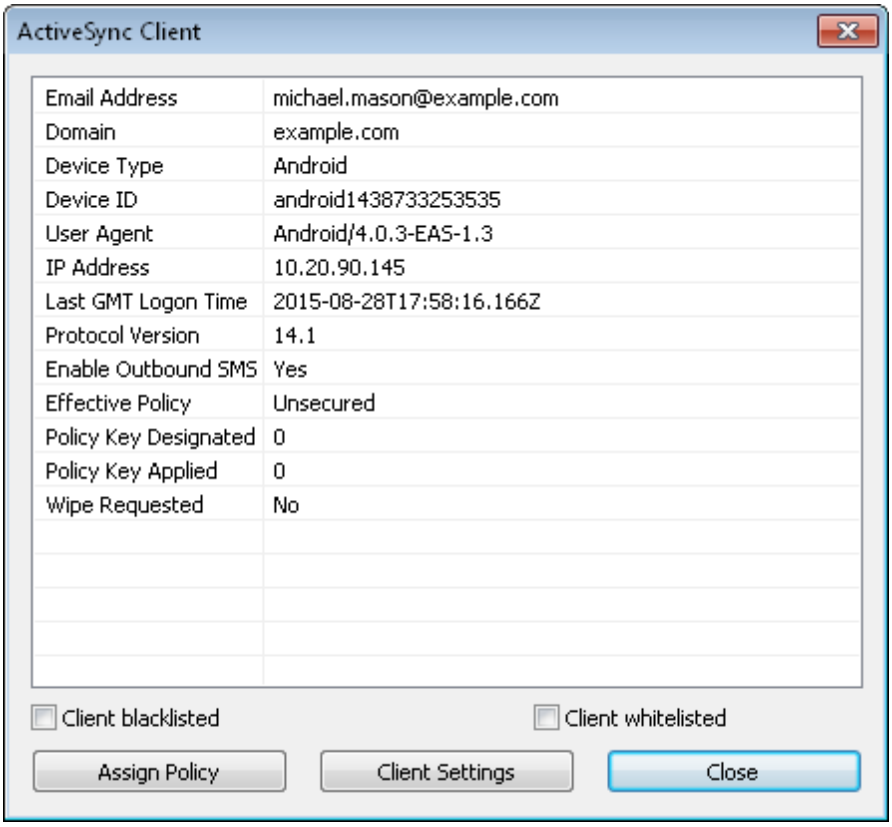
3.8.1.6 Clients



This screen contains an entry for each ActiveSync device associated with your system. Double-click any entry to see more details about the device.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Details



Select an entry and click **Details** (or double-click the entry) to open the Client Details dialog. On this screen you can view information about the device, assign a policy, access its client settings, or add the device to the blacklist or whitelist 308.

Device Settings

Select a device and click **Settings** to manage the Client Settings for the device. By default these settings are inherited from the account's 303 Client Settings screen. See Managing a Device's Client Settings below.

Assigning an ActiveSync Policy

To assign a Policy 284 to the device:

1. Select a device from the list.
2. Click **Assign Policy**. This opens the Apply Policy dialog.
3. Click the Assigned Policy drop-down list and choose the desired policy.
4. Click **OK**.

Statistics

Click **Statistics** to open the Device Statistics dialog, containing various usage stats for the device.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Reset Stats

If you wish to reset the device's stats, click **Reset Stats**, and **Ok** to confirm the action.

Removing an ActiveSync Device

To remove an ActiveSync device, select the device and click *Remove*. This will remove the device from the list and delete all synchronization information related to it in MDaemon. Therefore if in the future the account uses ActiveSync to synchronize the same device, MDaemon will treat the device as if it had never before been used on the server; all device data will have to be re-synchronized with MDaemon.

Full Wiping an ActiveSync Device

To do a Full Wipe on an ActiveSync device, select the device from the list and click *Full Wipe*. The next time the device connects, MDaemon will tell it to erase all data, or restore itself to its factory default state. Depending on the device, this may remove everything on it, including downloaded apps. Further, as long as the device's ActiveSync entry exists in MDaemon, it will be wiped again if it ever connects again to MDaemon in the future. If you no longer wish to wipe the device when it connects (for example, if a lost device is recovered and you wish to use it again with the account) then you must first use the *Remove* option above to remove the device from MDaemon.

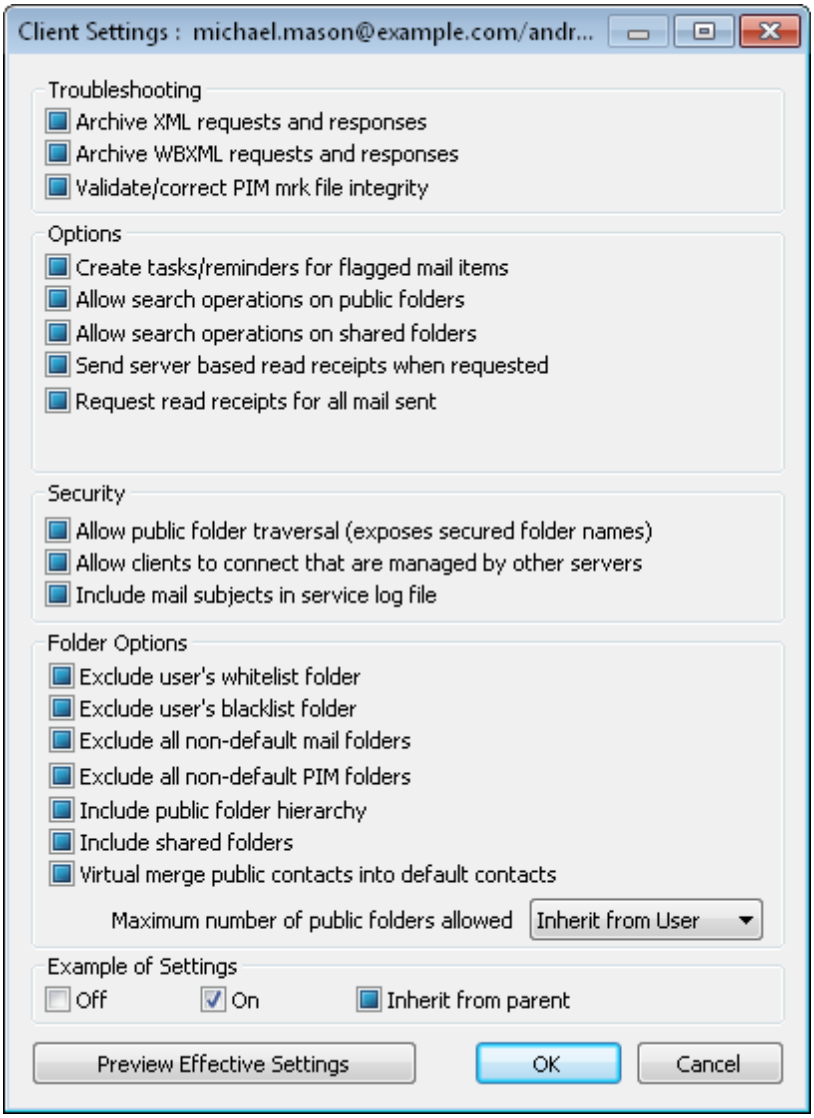
Data/Soft Wiping an ActiveSync Device

The *Data Wipe* (or *Soft Wipe*) option is similar to the *Full Wipe* option explained above, but instead of wiping all data, it will wipe only the account's data, such as its emails, calendar entries, contacts, and the like. The rest, such as apps, photos or music is left alone.

Managing a Device's Client Settings

The device-level Client Settings screen allows you to manage settings for a specific device.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.


Client Settings : michael.mason@example.com/andr...
Troubleshooting
Archive XML requests and responses
Archive WBXML requests and responses
Validate/correct PIM mrk file integrity
Options
Create tasks/reminders for flagged mail items
Allow search operations on public folders
Allow search operations on shared folders
Send server based read receipts when requested
Request read receipts for all mail sent
Security
Allow public folder traversal (exposes secured folder names)
Allow clients to connect that are managed by other servers
Include mail subjects in service log file
Folder Options
Exclude user's whitelist folder
Exclude user's blacklist folder
Exclude all non-default mail folders
Exclude all non-default PIM folders
Include public folder hierarchy
Include shared folders
Virtual merge public contacts into default contacts
Maximum number of public folders allowed
Inherit from User
Example of Settings
Off
On
Inherit from parent
Preview Effective Settings
OK
Cancel

By default all of the options on this screen are set to "Inherit from user," which means that each option will take its setting from the corresponding option on the account's Client Settings 303 screen. Any changes made to the settings on that screen will be reflected on this screen. Conversely, any changes you make to this screen will override the account-level setting for this device.

Troubleshooting

Archive [XML | WBXML] requests and responses
Use the *Archive XML...* and *Archive WBXML...* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

UIDs or empty required fields. The global option is disabled by default.

Options

Create Tasks/Reminders for flagged mail items
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email. This is disabled by default.

Allow search operations on Public Folders
Allows the client to search the Public Folders 218 to which it has access. This is allowed by default.

Allow search operations on Shared Folders
Allows the client to search the Shared Folders 547 to which it has access. This is allowed by default.

Send server based read receipts when requested.
Enable this option if you want the server to support read confirmation requests an issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Request read receipts for all mail sent
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Maximum number of clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default.

Security

Allow Public Folder traversal (exposes secured folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 220 for both the subfolder (i.e. child folder) and all parent public folders 218 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Allow clients to connect that are managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Disable this option if you do not wish to allows those clients to connect.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Include mail subjects in service log file
Enable this option if you wish to include each message's Subject header in the ActiveSync log file. This is not recommended, and this option is disabled by default.

Folder Options

Exclude user's [whitelist/blacklist] folder
By default the user's whitelist and blacklist contact folders are not synced with devices. They are generally only used by MDaemon, to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Exclude all non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Exclude all non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include Public Folder hierarchy
Check this box if you want the public folders 218 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Include shared folders
Check this box if you want the shared folders 87 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Virtual merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Maximum number of Public Folders allowed
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 292, accounts 303, and clients 297). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are

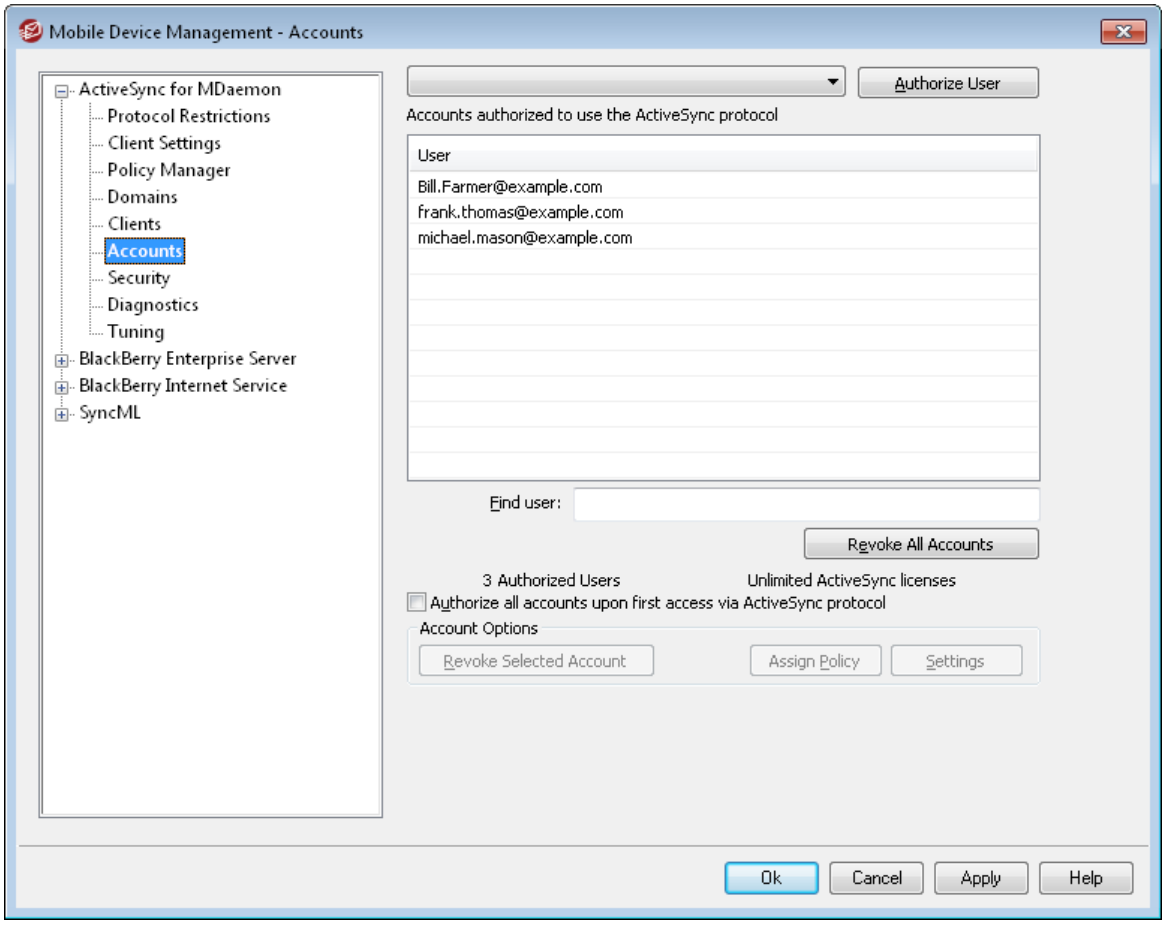
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

currently being applied to the displayed screen.

See:

ActiveSync » Client Settings 280
ActiveSync » Domains 292
ActiveSync » Accounts 303

3.8.1.7 Accounts



Use this screen to designate the accounts that are authorized to use ActiveSync. You can manually authorize or revoke accounts, or set MDaemon to authorize them automatically one at a time as each account connects using ActiveSync.

Manually authorizing or revoking accounts

To manually authorize an account to use ActiveSync, choose the account from the drop-down list at the top of the screen and click **Authorize User**. To revoke an account's authorization, select it from the list and click **Revoke Selected Account**.

If you have enabled the option to *Authorize all accounts upon*

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

> *first access via ActiveSync protocol*, revoking an account's access will remove it from the list, but the next time a device connects for the account it will be authorized again.

Revoke All Accounts

Click this button to revoke all accounts currently authorized to use ActiveSync.

Authorize all accounts upon first access via ActiveSync

Check this box if you wish to authorize accounts automatically, one at a time, whenever they connect to MDaemon using ActiveSync.

Assigning an ActiveSync Policy

To assign a Policy 284 to the account:

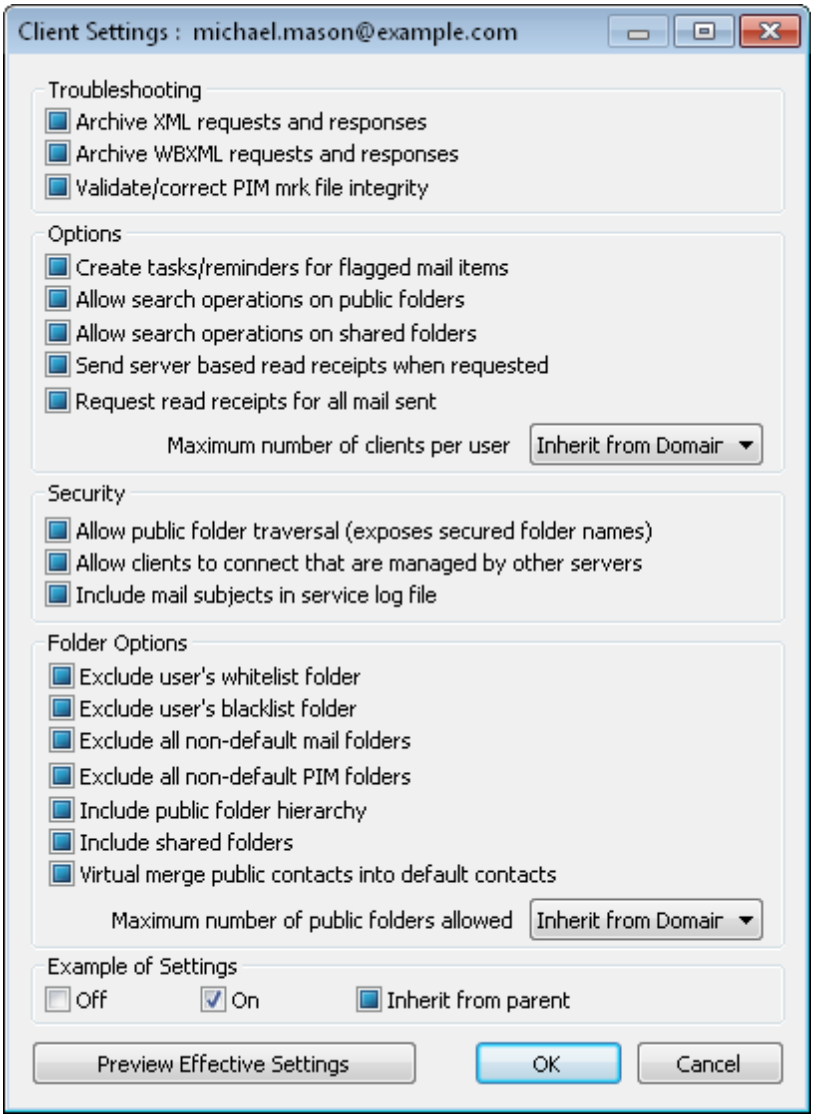
1. Select an account from the list.
2. Click **Assign Policy**. This opens the Apply Policy dialog.
3. Click the Assigned Policy drop-down list and choose the desired policy.
4. Click **OK**.

This policy will be assigned to any new device that connects for this account.

Settings

Select an account and click **Settings** to manage the Client Settings for the account. These settings will be applied to any ActiveSync clients that connect for the account.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.


Client Settings : michael.mason@example.com
Troubleshooting
Archive XML requests and responses
Archive WBXML requests and responses
Validate/correct PIM mrk file integrity
Options
Create tasks/reminders for flagged mail items
Allow search operations on public folders
Allow search operations on shared folders
Send server based read receipts when requested
Request read receipts for all mail sent
Maximum number of clients per user
Inherit from Domair
Security
Allow public folder traversal (exposes secured folder names)
Allow clients to connect that are managed by other servers
Include mail subjects in service log file
Folder Options
Exclude user's whitelist folder
Exclude user's blacklist folder
Exclude all non-default mail folders
Exclude all non-default PIM folders
Include public folder hierarchy
Include shared folders
Virtual merge public contacts into default contacts
Maximum number of public folders allowed
Inherit from Domair
Example of Settings
Off
On
Inherit from parent
Preview Effective Settings
OK
Cancel

By default all of the options on this screen are set to "Inherit from Domain," which means that each option will take its setting from the corresponding option on the domain's Client Settings 292 screen. Any changes made to the settings on that screen will be reflected on this screen. Conversely, any changes you make to this screen will override the domain-level setting for this account.

Troubleshooting

Archive [XML | WBXML] requests and responses
Use the *Archive XML...* and *Archive WBXML...* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

UIDs or empty required fields. The global option is disabled by default.

Options

Create Tasks/Reminders for flagged mail items
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email. This is disabled by default.

Allow search operations on Public Folders
Allows the client to search the Public Folders 218 to which it has access. This is allowed by default.

Allow search operations on Shared Folders
Allows the client to search the Shared Folders 547 to which it has access. This is allowed by default.

Send server based read receipts when requested.
Enable this option if you want the server to support read confirmation requests an issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Request read receipts for all mail sent
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Maximum number of clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default.

Security

Allow Public Folder traversal (exposes secured folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 220 for both the subfolder (i.e. child folder) and all parent public folders 218 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Allow clients to connect that are managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Disable this option if you do not wish to allows those clients to connect.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Include mail subjects in service log file
Enable this option if you wish to include each message's Subject header in the ActiveSync log file. This is not recommended, and this option is disabled by default.

Folder Options

Exclude user's [whitelist/blacklist] folder
By default the user's whitelist and blacklist contact folders are not synced with devices. They are generally only used by MDaemon, to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Exclude all non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Exclude all non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include Public Folder hierarchy
Check this box if you want the public folders 218 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Include shared folders
Check this box if you want the shared folders 87 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Virtual merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Maximum number of Public Folders allowed
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 292, accounts 303, and clients 297). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are

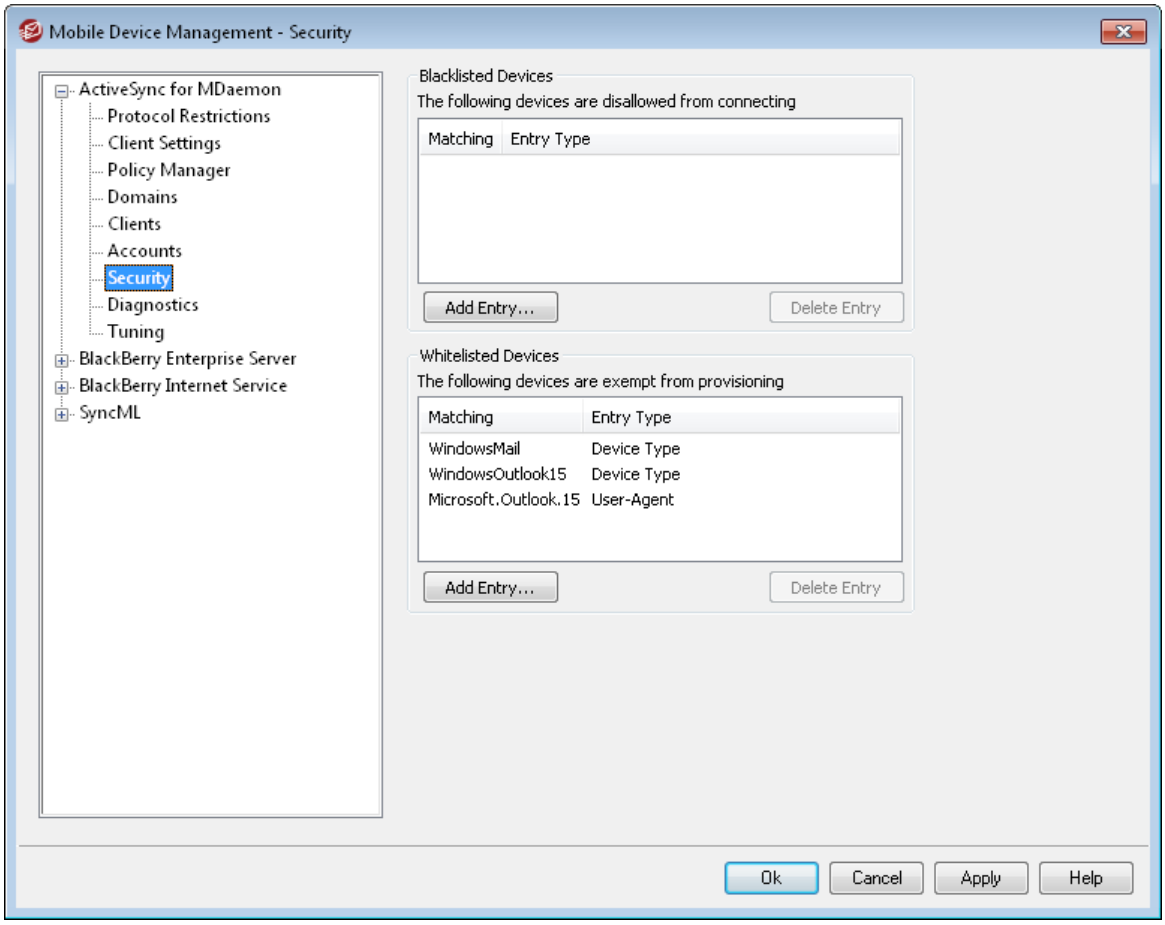
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

currently being applied to the displayed screen.

See:

ActiveSync » Client Settings 280
ActiveSync » Domains 292
ActiveSync » Clients 297

3.8.1.8 Security



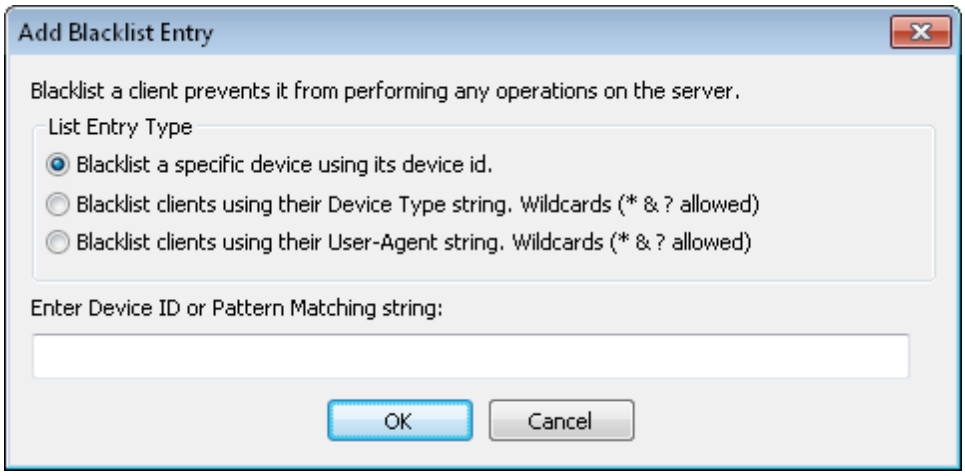
Blacklisted Devices

Use this option to prevent a specific Device Type, Device ID, or User Agent from accessing MDaemon's ActiveSync server.

Adding a Blacklist Entry

To add an entry to the list, click **Add Entry**, specify the device info, and click **Ok**. You can obtain the device info from the device itself or from the ActiveSync log files if the device has connected to MDaemon's ActiveSync server.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.


Add Blacklist Entry
Blacklist a client prevents it from performing any operations on the server.
List Entry Type
Blacklist a specific device using its device id.
Blacklist clients using their Device Type string. Wildcards (* & ? allowed)
Blacklist clients using their User-Agent string. Wildcards (* & ? allowed)
Enter Device ID or Pattern Matching string:
OK
Cancel

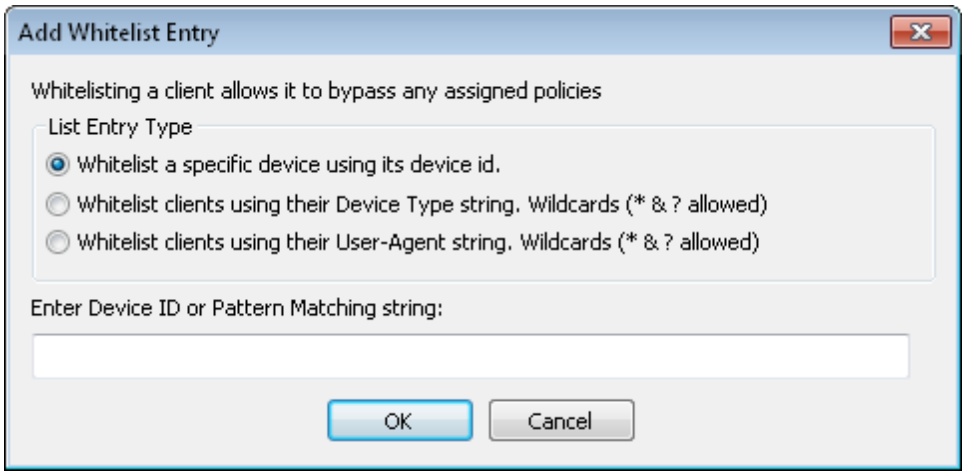
You can blacklist a device easily from the Device Details 297 dialog, accessed from the Clients screen. Select a client, click **Details**, and then click **Client blacklisted**.

Deleting a Blacklist Entry
To delete entries, select one or more entries from the list and click **Delete Entry**. You will be asked to confirm the action before they are deleted.

Whitelisted Devices

Use this option to exempt a specific Device Type, Device ID, or User Agent from provisioning, or policy 284 restrictions.

Adding a Whitelist Entry
To add an entry to the list, click **Add Entry**, specify the device info, and click **Ok**. You can obtain the device info from the device itself or from the ActiveSync log files if the device has connected to MDaemon's ActiveSync server.


Add Whitelist Entry
Whitelisting a client allows it to bypass any assigned policies
List Entry Type
Whitelist a specific device using its device id.
Whitelist clients using their Device Type string. Wildcards (* & ? allowed)
Whitelist clients using their User-Agent string. Wildcards (* & ? allowed)
Enter Device ID or Pattern Matching string:
OK
Cancel

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

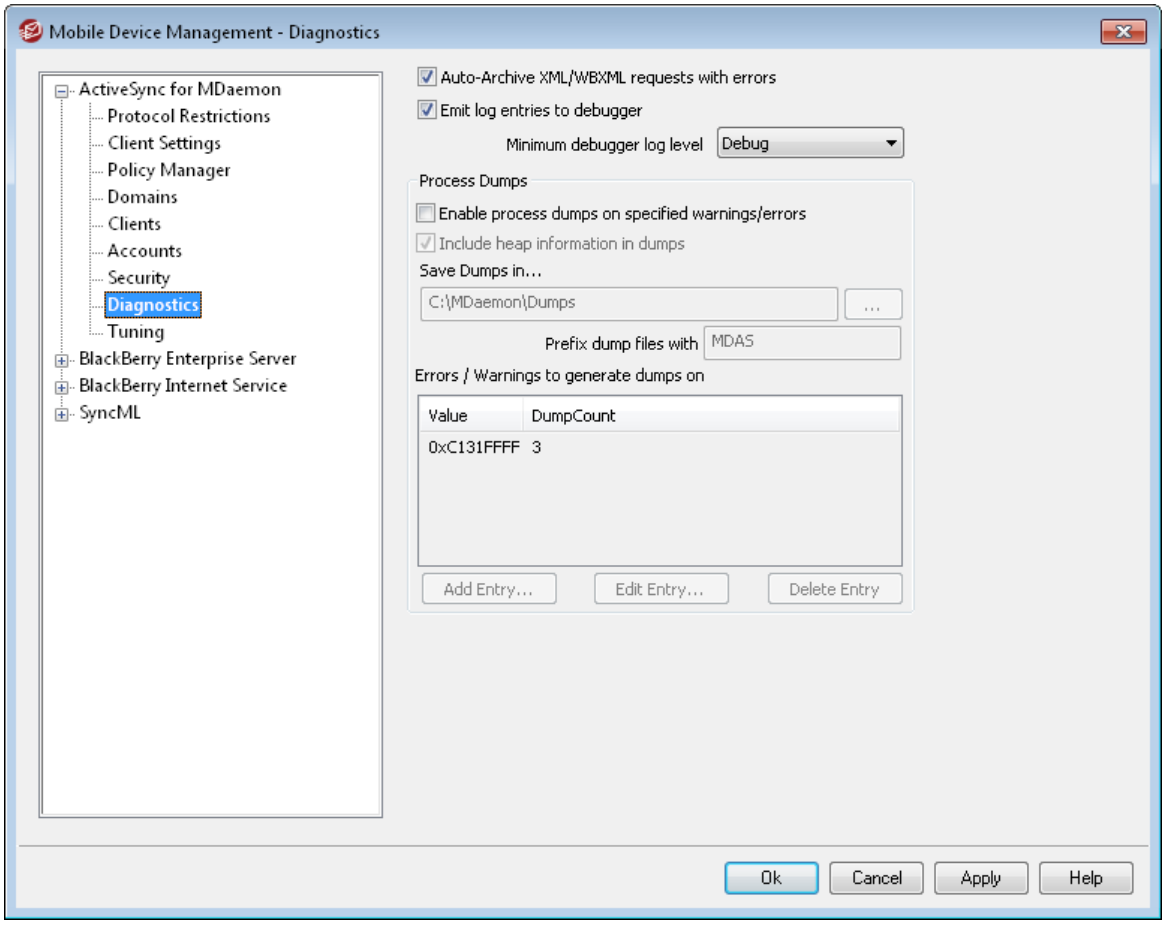
You can whitelist a device easily from the Device Details 297 dialog, accessed from the Clients screen. Select a client, click **Details**, and then click **Client whitelisted**.

Deleting a Whitelist Entry
To delete entries, select one or more entries from the list and click **Delete Entry**. You will be asked to confirm the action before they are deleted.

See:

ActiveSync » Clients 297

3.8.1.9 Diagnostics



This screen contains advanced options that in most cases will not need to be used unless you are attempting to diagnose a problem or dealing with technical support, and by default it is hidden from the Mobile Device Management interface. If you want it to be visible, click **Enable advanced management options** on the ActiveSync for MDaemon 276 screen.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Auto-Archive XML/WBXML requests with errors
In the event that you have turned off the options to *Archive [XML | WBXML] requests and responses* on the Client Settings 280 screen, this option will still archive problematic XML or WBXML requests. Only requests that cause errors will be archived. This option is enabled by default.

Emit log entries to debugger
If you have a Debug monitor (such as WinDbg or DbgCiew) attached to the process, this option causes the logging mechanism to emit all log entries to the debugger so that you can see what is happening in real time.

Minimum debugger log level
This is the minimum level of logging to emit to the debugger. The available log levels are the same as those outlined on the Tuning 312 screen.

Process Dumps

Enable process dumps on specified warnings/errors
Enable this option if you want the ActiveSync service to generate process dumps whenever a specific warning or error occurs that you have designated below.

Include heap information in dumps
By default, heap information is included in the process dumps. Clear this checkbox if you do not with to include it.

Save Dumps in...
The is the location to save the dump files.

Prefix dump files with
Process dump filenames will begin with this text.

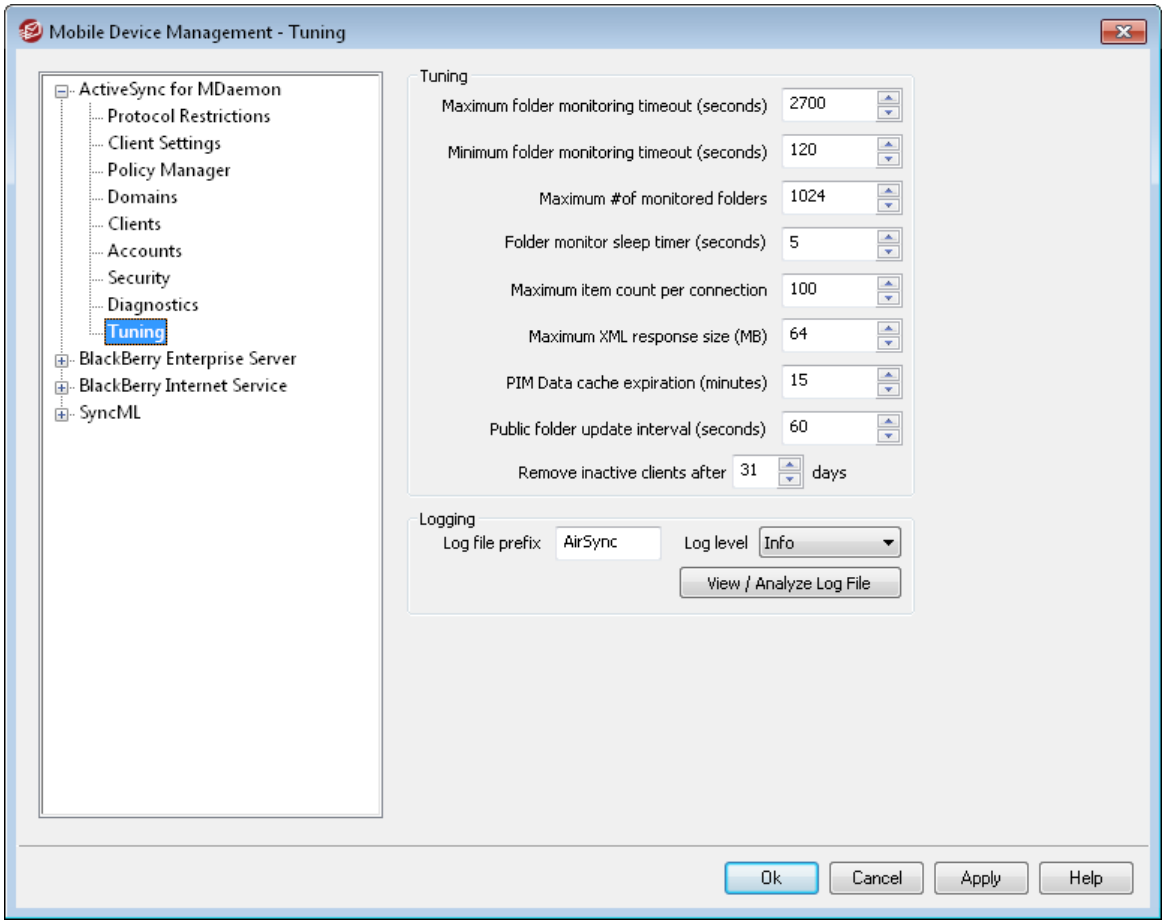
Errors/Warnings to generate dumps on
Use the *Add/Edit/Delete Entry...* options to manage the list of errors or warnings that will trigger process dumps. For each entry you can specify the number of process dumps allowed before it will be deactivated.

See:

ActiveSync » Tuning 312

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.8.1.10 Tuning



This screen contains advanced options that in most cases will not need to be adjusted, and by default it is hidden from the Mobile Device Management interface. If you want it to be visible, click **Enable advanced management options** on the ActiveSync for MDaemon 276 screen.

Settings

Maximum folder monitoring timeout seconds (seconds)
This is the maximum amount of time that MDaemon ActiveSync Service (MDAS) will wait while monitoring a folder before returning a response to the client. The default value is 2700 seconds (i.e. 45 minutes).

Minimum folder monitoring timeout seconds (seconds)
This is the minimum amount of time that MDAS will wait while monitoring a folder before returning a response to the client. The default value is 120 seconds. If necessary you can reduce the number of connections that are made to the server by raising this value, since it would cause the client to connect less often due to the wait time involved being longer.

Maximum # of monitored folders
This is the maximum number of folders that each ActiveSync client is allowed to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

monitor for changes. The default is 1024.

Folder monitor sleep timer (seconds)
This is the number of seconds that the ActiveSync service will wait between folder monitoring occurrences. This is set to 5 seconds by default.

Maximum item count per connection
This is the maximum number of items that the ActiveSync service will return to the client in response to a Sync request. Using a lower value in this option can reduce memory usage on a busy server, but it will require more connections and bandwidth. It can also decrease battery life because devices may need to make more requests to get all changes during a sync. Higher values in this option increase memory usage and are more susceptible to communication errors. The default value of 100 is generally a good compromise. It is worth noting, however, that clients will specify the value that they prefer, which could effectively lower this value for some clients. If a client requests a value greater than the maximum, then the maximum will be used.

Maximum XML response size (MB)
This is the maximum allowable size of a response to a Sync request from a client. Prior to processing a given item for server-to-client synchronization, the current size of the response is checked and if it is greater than or equal to this value, the collection is flagged that there are more changes available, and we cease adding more items to the response. This is useful with servers that regularly contain a lot of large attachments in their email.

PIM Data cache expiration (minutes)
Since Contacts, Documents, Events, and other PIM data is often static, getting only occasional updates from clients, MDAS caches this data to reduce disk activity. It is, however, automatically reloaded whenever the data changes on disk. This value controls how long to cache the user's data since the last time it was accessed.

Public folder update interval (seconds)
This is the number of seconds MDAS will wait before updating Public Folders. The default interval is 60 seconds.

Remove inactive clients after [xx] days
This is the number of days that an ActiveSync device 297 can go without connecting to MDAS before it will be removed. When the device is removed, its configuration and access settings are discarded. If the device ever connects again, MDaemon will respond as if it is a new device that has never been used on the server. It will be forced to reprovision if a policy is in place for the domain 292 or account 303, perform an initial folder sync, and re-sync all subscribed folders. This option can help keep your server free from maintaining information for old and unused devices. The option is set to 31 days by default.

Logging

Log file prefix
The filenames of MDAS log files will start with this text. "AirSync" is the default prefix.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Log level
ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Debug	This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.
Info	Moderate logging. Logs general operations without details. This is the default log level.
Warning	Warnings, errors, critical errors, and startup/shutdown events are logged.
Error	Errors, critical errors, and startup/shutdown events are logged.
Critical	Critical errors and startup/shutdown event are logged.
None	Only startup and shutdown events are logged.

View/Analyze Log File
Click this button to open the ActiveSync log file viewer. By default the ActiveSync logs are stored in: "..\MDaemon\Logs\"

See:

ActiveSync » Diagnostics 310

3.8.2 BlackBerry Enterprise Server

MDaemon Pro is equipped with a BlackBerry Enterprise Server, which makes it possible for your users to synchronize their MDaemon/WorldClient email, calendar, and other personal information management (PIM) data with their BlackBerry smartphones. BlackBerry platform support also makes it possible for you to set security polices for user devices and even erase a device should it be lost or stolen.

MDaemon's BlackBerry Enterprise Server features include:

- No need for third-party sync clients. Each user's data is synchronized using software already present on all BlackBerry devices.
- MDaemon/WorldClient email (including mail folders) is synchronized with the device in both directions. Therefore whether mail is read, moved, deleted, etc. on the device or the server it will be synchronized on both.
- Two-way Calendar synchronization. For example, if you create a new appointment, set a reminder, or modify an appointment on either the device or within WorldClient it will be synchronized in both places.
- Two-way tasks and notes synchronization.
- Global address book lookup.
- Scheduling with free/busy.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

- Limited BlackBerry device policy support, so that you can set device policies such as: require passwords, expiring passwords, encrypt media files, and more.
- Set different policies for individual domains or users.
- Support for BlackBerry Balance. BlackBerry Balance allows for the separation of work and personal information on BlackBerry devices. BlackBerry Balance is only supported on BlackBerry devices running OS 6.0 MR2 or higher.
- Use the BlackBerry MDS Connection Service (MDS-CS) for behind-the-firewall access to files and web applications from BlackBerry devices. This will, for example, allow you to access your private Intranet without a VPN connection.
- Remotely change the device's password and lock it.
- Erase all data from the device, for example if it is lost or stolen.
- Backup and Restore options for your BlackBerry Enterprise Server database.

MDaemon's main BlackBerry Enterprise Server options are located at: Setup » BlackBerry... » BlackBerry Enterprise Server, and the account-specific options are located on the BlackBerry Enterprise Server 553 screen of the Account Editor.

BlackBerry Enterprise Server is not available in some countries and regions.

BlackBerry Dialog

The BlackBerry Enterprise Server section of the BlackBerry dialog has the following screens:

Status 318 — You can enable/disable the BlackBerry Enterprise Server from this screen and see the status of its various components and services. Your unique Server Routing Protocol (SRP) information in also displayed here, including your SRP ID and Key.

Policies 319 — This screen is where you will create and manage the IT policies that you will assign to activated BlackBerry devices. Polices control various things such as whether or not the device must be secured by a password or its files encrypted.

Domains 326 — Use the options on this screen to choose the default policy that will be assigned to each domain's new accounts. You can also apply a policy to a domain's existing accounts.

MDS-CS 327 — The BlackBerry Mobile Data System Connection Service (MDS-CS) permits behind-the-firewall access to files and web applications from BlackBerry devices. It receives and responds to web requests from the BlackBerry Browser and other BlackBerry Applications, and sends login requests so that users can view Internet and Intranet content on their BlackBerry devices.

Devices 328 — This screen lists all BlackBerry enabled accounts and their current state: activated or not activated. Activated accounts also list the activated device's PIN. Further, there is a button on the bottom of the screen that you can use to initiate a slow sync of all activated accounts. This resynchronizes all

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

account data, ensuring that the data on the devices matches the data in MDaemon.

Backup/Restore 329 — You can manually backup your BlackBerry Enterprise Server database from this screen and specify how many nightly backup files to save.

Settings 330 — With this screen you can set the BlackBerry Enterprise Server services to stop when MDaemon stops, configure logging options, and set several synchronization options for email and calendar data.

BlackBerry Device Activation

In order to begin using MDaemon's BlackBerry Enterprise Server features an account must "activate" a BlackBerry device with MDaemon. To do this complete the following steps.

In MDaemon:

1. Go to: Setup » BlackBerry... » BlackBerry Enterprise Server » Status.
2. Click **Enable BlackBerry Enterprise Server** if it is not already enabled.
3. If you need to create a custom policy for the device, click **Policies** 319 in the left pane to do so.
4. Click **OK**.
5. Go to: Accounts » Account Manager..., and double-click the account that you wish to allow to activate a device.
6. Click **BlackBerry Enterprise Server** 553 in the left pane of the Account Editor.
7. Click **Enable BlackBerry device synchronization**.
8. Choose a policy from the drop-down list.
9. Click **OK**.

On the user's device:

1. Disable or remove any third-party sync clients (such as a SyncML client) currently in use to synchronize data with the MDaemon account.
2. If the device is configured to use the BlackBerry Internet Service (BIS) to get email from the account, go to the device's email setup and remove that account.
3. If there are any existing calendar entries on the device, you must either wipe the device or reset the calendar. Otherwise existing calendar data on the MDaemon server may not be sent to the device. Always backup your device data before doing this. **Note:** if you choose to reset the calendar rather than wipe the device, the reset may be performed after activation. See **Resetting the Device Calendar** 333 for more information.

Note: Failure to ensure that Steps 1 and 2 above are completed may result in duplicates of email, calendar entries, or other PIM data on the device.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

In WorldClient, the user must:

1. Log in to WorldClient.
2. Go to: Options » BlackBerry Management.
3. Connect the device via a USB cable and follow the directions on the screen (requires Internet Explorer 6 or later).

   -or-

   Enter an activation password, click **Save**, and then activate the device over-the-air (OTA) directly from the device's Enterprise Activation screen — the user will enter the account's email address and activation password on the device. **Note:** Not all devices support OTA activation.
4. Sign out from WorldClient.

After initiating the activation process, whether via USB cable or OTA, it will continue on the device until finished. When the activation process is complete it will be paired with the MDaemon/WorldClient account. Within a short time data will begin to synchronize.

Depending on the device and operating system installed, activation may delete all data on the device, restoring it to its default settings before synchronizing it with MDaemon/ WorldClient. For this reason, before activating the device the user should use Desktop Manager or some other means to backup or export any data that he or she does not wish to lose.

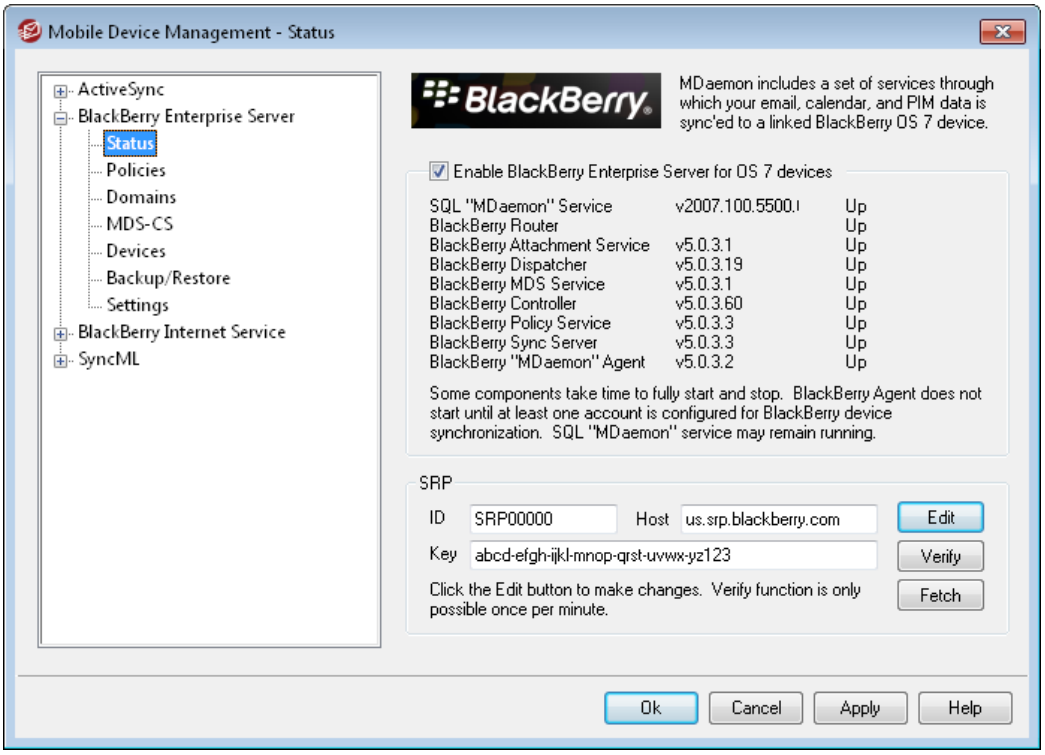
After a device is activated it may have various functionality changes or operating differences when compared to its state prior to BlackBerry Device Activation. The degree of difference depends on the device, OS, policy used, and whether or not it was previously activated on a different BlackBerry Enterprise Server.

See:

Account Editor » BlackBerry Enterprise Server 553
BlackBerry Internet Service 335

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.8.2.1 Status


Mobile Device Management - Status
ActiveSync
BlackBerry Enterprise Server
Status
Policies
Domains
MDS-CS
Devices
Backup/Restore
Settings
BlackBerry Internet Service
SyncML
BlackBerry
MDaemon includes a set of services through which your email, calendar, and PIM data is sync'ed to a linked BlackBerry OS 7 device.
Enable BlackBerry Enterprise Server for OS 7 devices
SQL "MDaemon" Service v2007.100.5500.1 Up
BlackBerry Router Up
BlackBerry Attachment Service v5.0.3.1 Up
BlackBerry Dispatcher v5.0.3.19 Up
BlackBerry MDS Service v5.0.3.1 Up
BlackBerry Controller v5.0.3.60 Up
BlackBerry Policy Service v5.0.3.3 Up
BlackBerry Sync Server v5.0.3.3 Up
BlackBerry "MDaemon" Agent v5.0.3.2 Up
Some components take time to fully start and stop. BlackBerry Agent does not start until at least one account is configured for BlackBerry device synchronization. SQL "MDaemon" service may remain running.
SRP
ID SRP00000 Host us.srp.blackberry.com Edit
Key abcd-efgh-ijkl-mnop-qrst-uvwx-yz123 Verify
Click the Edit button to make changes. Verify function is only possible once per minute.
Fetch
Ok
Cancel
Apply
Help

This screen is located at: `Setup » BlackBerry... » BlackBerry Enterprise Server » Status`. It is used to enable or disable the BlackBerry Enterprise Server and displays the status of its various components and services. Your unique Server Routing Protocol (SRP) information in also displayed here, including your SRP ID and Key.

Enable BlackBerry Enterprise Server

Check this box to enable the BlackBerry Enterprise Server (BES), starting its various services. Some of these components may take time to fully start or stop, and the SQL "MDaemon" Service may continue running when the BlackBerry Enterprise Server is stopped. The BlackBerry "MDaemon" Agent will not start until at least one account is enabled for BlackBerry device synchronization 553.

SRP

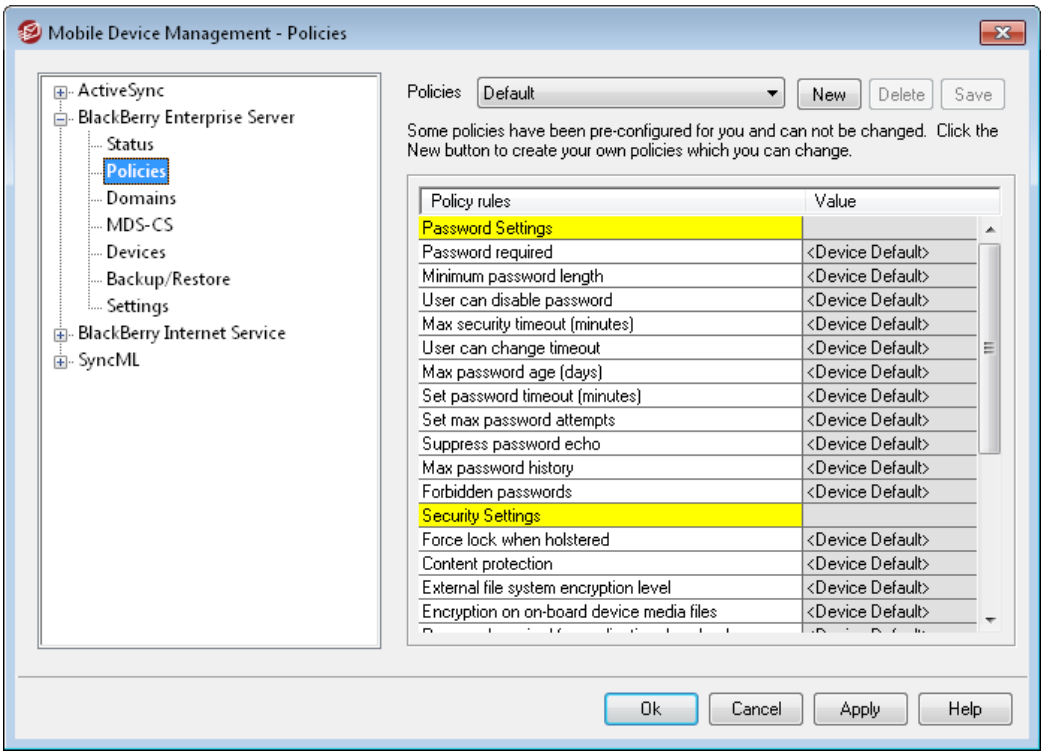
Server Routing Protocol (SRP) is used to authenticate and identify traffic between your MDaemon and your BlackBerry devices across the wireless network. This requires that your MDaemon have a unique SRP ID and SRP Key, which is obtained automatically during installation. Your SRP credentials are associated with your MDaemon server and cannot be used by any other server. You should not need to edit this information, but if it is necessary to do so then an **Edit** button is provided. You can also click **Verify** to confirm that your SRP credentials are valid.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

BlackBerry Enterprise Server 314
Account Editor » BlackBerry Enterprise Server 553

3.8.2.2 Policies



When a BlackBerry device is activated on MDaemon, a designated policy is pushed to that device. Policies are sets of rules that govern what is required or permitted on a device. They allow you to do things like require passwords, force the device to lock when holstered, encrypt files on the device, and more. Policies can be assigned to domains and to individual accounts. Use the Domains 326 screen to assign policies to domains, or use the BlackBerry Enterprise Server 553 screen on the Account Editor to assign them to specific accounts. MDaemon is equipped with three pre-configured policies, and you can create your own custom policies.

After a device is activated it may have various functionality changes or operating differences when compared to its state prior to BlackBerry Device Activation. The degree of difference depends on the device, OS, policy used, and whether or not it was previously activated on a different BlackBerry Enterprise Server.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Pre-configured Policies

There are three pre-configured policies that cannot be edited or removed:

Default
This policy causes the BlackBerry device to use standard BlackBerry Enterprise Server defaults for all settings. This is a standard "out-of-the-box" and "under the control of a BlackBerry Enterprise Server" policy configuration.

Password Required
This policy is like *Default* except that it sets the *Password Required* rule to `YES` and the *User can disable password* rule to **No** (see rule descriptions below). Devices with this policy must be secured by a password.

Expiring Passwords
This policy is like *Password Required* but also sets the *Max password age (days)* rule to `30`. The password on the device will have to be changed at least every 30 days.

Creating a Custom Policy

To create a custom policy:

1. Click **New**.
2. Enter a name for the policy.
3. Click **OK**.
4. Set the various policy rules as desired.
5. Click **Save**.

Policy Rules

The following is a list of all policy rules that you can set when creating or editing a custom policy.

Password Settings

Contains policy rules that apply to BlackBerry device password settings.

Password required
Specify whether the BlackBerry device requires a password. Set this rule to **YES** to require the user to enter a password to unlock the BlackBerry device.

Rule dependency: If you enable this rule, you should set the *User can disable password* rule to **NO** to prevent the BlackBerry device user from disabling this rule.

Minimum password length
Type the minimum required length, in characters, of the BlackBerry device password. This rule only controls the minimum password length, not the maximum password length. The maximum password length is 32 characters.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

The valid range for the value of this rule is 4 through 14.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

User can disable password
Specify whether the user can disable the requirement for a BlackBerry device password. Set this rule to **NO** to prevent users from disabling the password requirement on the BlackBerry device.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

Max security timeout (minutes)
Specify the maximum time, in minutes, that a BlackBerry device user can set as the security timeout value (the number of minutes of BlackBerry device user inactivity allowed before the security timeout occurs and the device requires the user to type the BlackBerry device password to unlock it). The BlackBerry device user can set any timeout value that is less than or equal to the maximum value, unless you set the *User can change timeout* rule value to **NO**. The maximum security timeout value available by default on the BlackBerry device is 60 minutes. The valid range for the value of this rule is **10-480** minutes.

Note: Use the *Set Password Timeout (minutes)* rule if you wish to set a specific timeout value.

Rule dependency: The BlackBerry device uses this policy rule only if the *Password required* rule is set to **YES**.

User can change timeout
Specify whether the BlackBerry device user can change the security timeout. If set to **YES**, the user can set the timeout to any available value up to the limit set in the *Max security timeout (minutes)* rule. Set this rule to **NO** if you wish to prevent the user from changing the timeout value. If no value is set then a default value of **YES** is used.

Max password age (days)
Type the number of days until a BlackBerry device password expires and the BlackBerry device prompts the user to set a new password. The valid range for the value of this rule is **0-65535** days. **Note:** Set this rule to **0** to prevent the BlackBerry device password from expiring.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

Set password timeout (minutes)
Specify the amount of time, in minutes, of BlackBerry device user inactivity

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

allowed before the security timeout occurs and the BlackBerry device requires the user to type the password to unlock the BlackBerry device. The valid range for the value of this rule is **0-60**.

Note: The default security timeout interval is 2 minutes of inactivity for BlackBerry device software versions earlier than 4.7, and 30 minutes of inactivity for BlackBerry device software versions 4.7 and later.

Rule dependencies: The BlackBerry device uses this rule only if the *Password required* rule is set to **YES**. If you do not set the *User can change timeout* rule to **NO**, the BlackBerry device user can set the password timeout to one of a range of values. The maximum security timeout value available by default on the BlackBerry device is 60 minutes.

Set max password attempts
Set the number of password attempts (incorrect passwords entered) permitted on the BlackBerry device before the BlackBerry device data is erased and the BlackBerry device is disabled. The valid range for the value of this rule is **3-10** attempts. **10** attempts are allowed by default.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

Suppress password echo
Set this rule to **YES** to prevent the echoing (printing to the screen) of characters typed into the password screen after the user has entered a set number of incorrect passwords while attempting to unlock the device.

Note: You can use the *Set max password attempts* rule to designate the number of incorrect password attempts allowed before password echoing occur (if permitted).

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a password, set the *Password required* rule to **YES**.

Max password history
Set the maximum number of previous passwords against which the BlackBerry device can check new passwords to prevent reuse of the old passwords. The valid range for the value of this rule is **0-15** passwords. Set this rule to **0** to prevent the BlackBerry device from checking for reused passwords. If you do not set this rule, a default value of **0** will be used.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

Forbidden passwords
Type a list of comma-separated string values representing words that users are not permitted to use within their passwords.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Note: The BlackBerry device automatically prevents common letter substitutions. For example, if you include "password" in the forbidden passwords list, users cannot use "p@ssw0rd", "pa$zword", or "password123" on the BlackBerry device.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

Security Settings

Contains policy rules that apply to BlackBerry device security."

Force lock when holstered

Specify whether the BlackBerry device is security locked when placed in the holster. If you do not set this rule, a default value of **NO** will be used.

Content protection

Specify whether content protection is turned on.

When content protection is turned on, BlackBerry device content is always protected with the 256 bit AES encryption algorithm. If the BlackBerry device is locked when it receives content, the BlackBerry device randomly generates the content protection key (a 256 bit AES encryption key) and an ECC key pair, derives an ephemeral 256 bit AES encryption key from the BlackBerry device password, and uses the ephemeral key to encrypt the content protection key and the ECC private key.

Rule dependency: The BlackBerry device uses this policy rule only if the *Password required* rule is set to **YES**.

External file system encryption level

Specify the level of file system encryption that the BlackBerry device uses to encrypt files that it stores on an external file system. You can use this policy rule to require the BlackBerry device to encrypt an external file system, either including or excluding multimedia directories. If you do not set this rule, a default value of **Level 0** (i.e. Not Required) will be used.

You can set this rule to the following values:

Level 0: Not Required

Level 1: Encrypt to User Password (excluding multi-media directories)

Level 2: Encrypt to User Password (including multi-media directories)

Level 3: Encrypt to Device Key (excluding multi-media directories)

Level 4: Encrypt to Device Key (including multi-media directories)

Level 5: Encrypt to User Password and Device Key (excluding multi-media directories)

Level 6: Encrypt to User Password and Device Key (including multi-media directories)

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Encryption on on-board device media files
Specify whether the media files located on the on-board device memory will be encrypted to the user password and the device generated key if on-board device memory exists. If you set this rule to **Required** or **Disallowed** the user cannot change this setting on the device. If you do not set this rule, a default value of **Allowed** will be used.

Rule dependency: The BlackBerry device uses this policy rule only if the *Content protection strength* is set.

Password required for application download
Specify whether the BlackBerry device will prompt the user for their password prior to using the browser to download applications.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

Disable organizer data access for social networking apps
This rule specifies whether a BlackBerry device must prevent social networking applications from accessing organizer data such as contacts and calendar data. Set this to **NO** to grant social networking applications access to the address book, calendar, and other organizer data. This rule's default value is **YES**, social networking applications cannot access organizer data on the device.

BlackBerry Balance

Contains policies governing separation of work and personal data.

Enable separation of work content
Specify whether a BlackBerry device distinguishes between work data and personal data and whether the applications on the device can access work data.

If you do not set this rule, a default value of **NO** will be used.

Disable forwarding of work content using personal channels
Specify whether a BlackBerry device user can send work data to contacts using personal resources (for example, SMS text messaging, MMS messaging, or personal email accounts).

If you do not set this rule, a default value of **NO** will be used.

Rule dependency: This rule requires the *Enable separation of work* rule to be enabled.

Require work resources for conducting work activities
Specify whether a BlackBerry device must use work resources (for example, work email accounts or work calendars) when a BlackBerry device user conducts work activity (for example, sending an email message to a work

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

contact or scheduling a work appointment).

If you do not set this rule, a default value of **NO** will be used.

Rule dependency: This rule requires the *Enable separation of work* rule to be enabled.

Work domains
Type a list of comma-separated string values listing domain names that the BlackBerry device will identify as a work resource (for example: altn.com, example.com). Sub-domains are included automatically.

Other

Miscellaneous settings

Allow web-based software loading
Specify whether to allow a user to update the BlackBerry device software using the web-based software loading feature. If you do not set this rule, a default value of **NO** will be used.

MDS browser domains
Specify a list of web addresses that the BlackBerry device should retrieve using the BlackBerry browser. Separate multiple web addresses with a comma. If you wish to allow the BlackBerry browser to retrieve sub-domains of a web address then prefix the domain with a period. For example, type ".`example.com`" to allow for sub-domains of `example.com`, such as: `mail.example.com`, `www.example.com`, etc.

This rule applies only to Java-based BlackBerry devices version 4.2.0 and higher.

Policy author's name
Enter the name of the author of this policy.

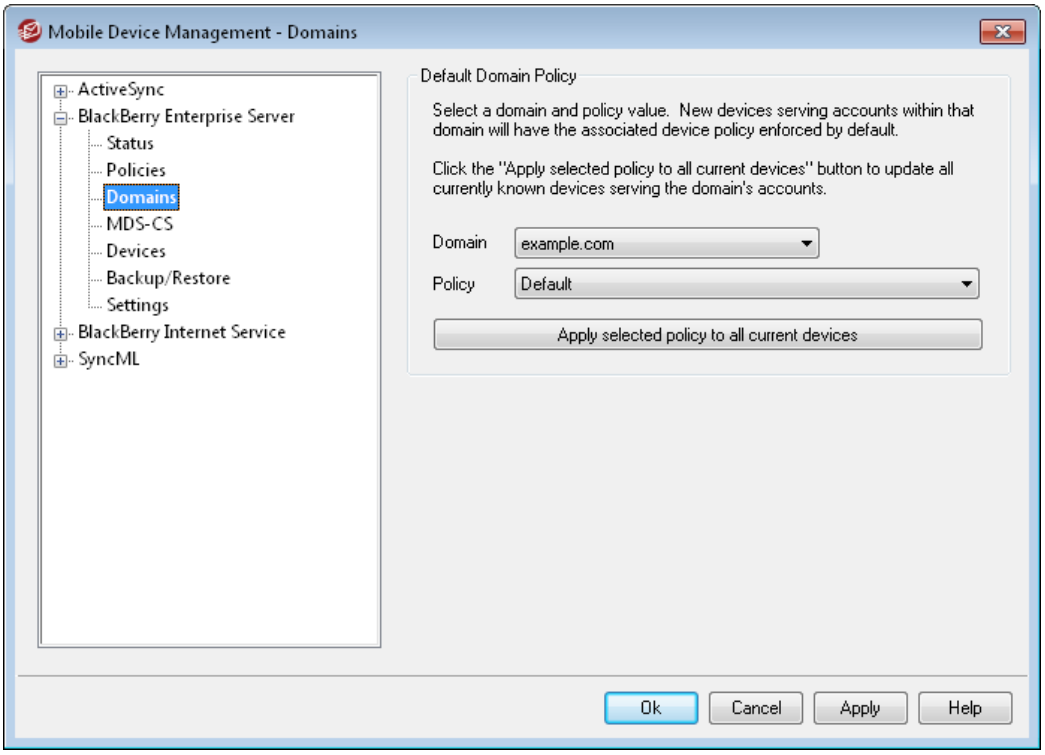
Policy description
Enter some text to describe this policy.

See:

BlackBerry Enterprise Server 314
Domains 326
Account Editor » BlackBerry Enterprise Server 553

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.8.2.3 Domains



Default Domain Policy

To designate the default policy[319] that will be assigned to each new BlackBerry activation on a particular domain, select the desired domain from the drop-down list, select the policy that you wish to assign to all new activations, and then click **OK**. Only new activations will have this policy assigned. Existing activations will not be changed.

Apply to all of the domain's activated accounts

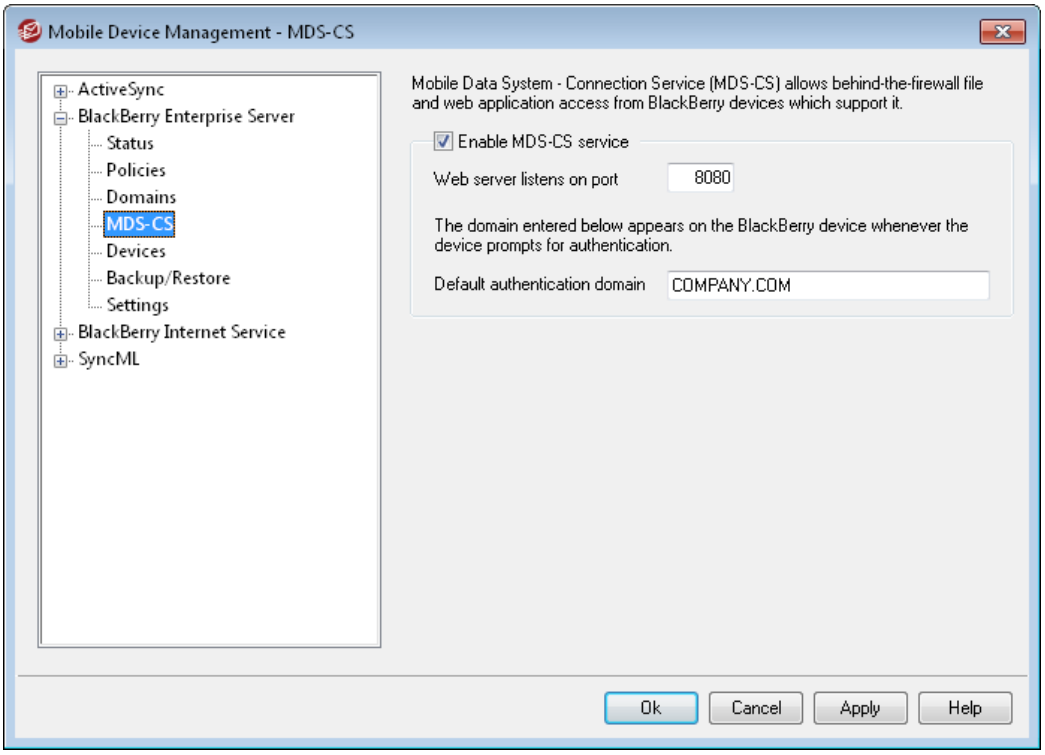
If you wish to apply a policy to all devices already activated on a domain, select a domain and policy from the drop-down lists and then click this button. The policy will be applied to **all** activated accounts on the domain—even to those accounts that have had a different policy assigned to them on the Account Editor's BlackBerry Enterprise Server[553] screen.

See:

BlackBerry Enterprise Server[314]
Account Editor » BlackBerry Enterprise Server[553]

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.8.2.4 MDS-CS



BlackBerry® Mobile Data System Connection Service (MDS-CS)

MDS-CS permits behind-the-firewall access to files and web applications from BlackBerry devices. It receives and responds to web requests from the BlackBerry Browser and other BlackBerry Applications, and sends login requests so that users can view Internet and Intranet content on their BlackBerry devices. This will, for example, allow you to access your private Intranet without a VPN connection.

You can find more information about MDS-CS at BlackBerry.com, but please note that not all of the features and capabilities documented there are supported by MDaemon.

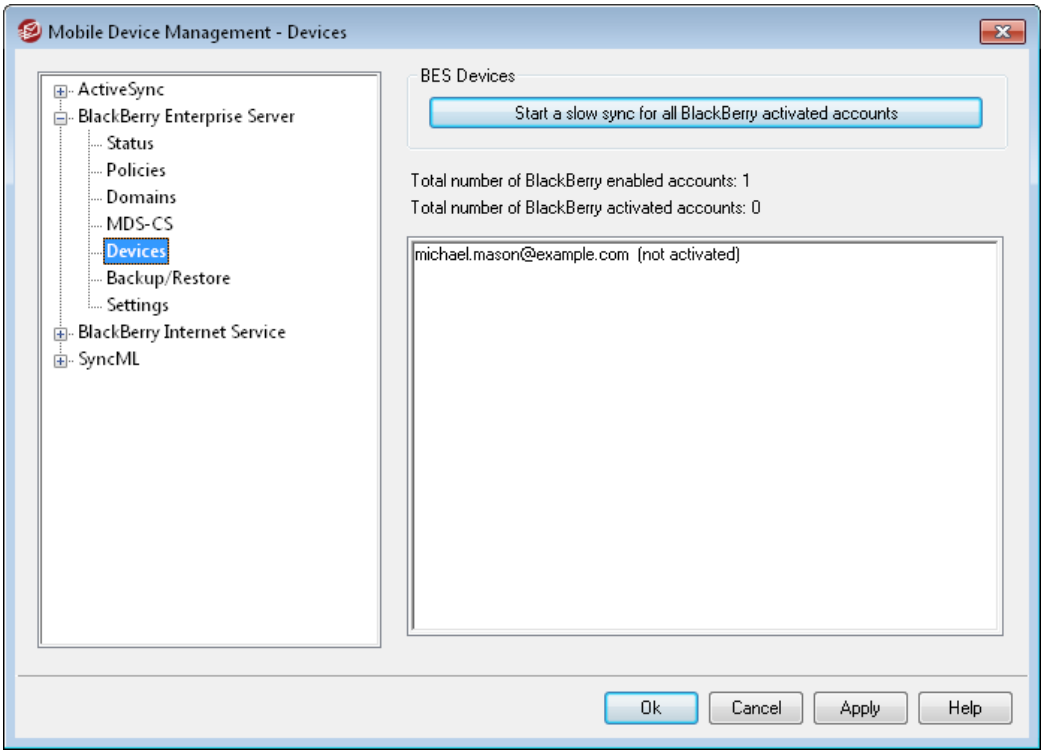
Enable MDS-CS service
Clear this check box if you do not wish to run the BlackBerry MDS Connection Service.

Web server listens on port
This is the port on which the web server will listen for connections from your BlackBerry devices.

Default authentication domain
This is the domain value that will appear on the BlackBerry device anytime the device prompts the user for authentication related to MDS-CS activities.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.8.2.5 Devices



BES Devices

This screen lists all accounts that have been enabled for BlackBerry device synchronization, and their current state: activated or not activated. Activated accounts also display the activated device's PIN. Under the account list is a counter that tells you the number of accounts that are enabled for BlackBerry device synchronization and the number of accounts that are activated.

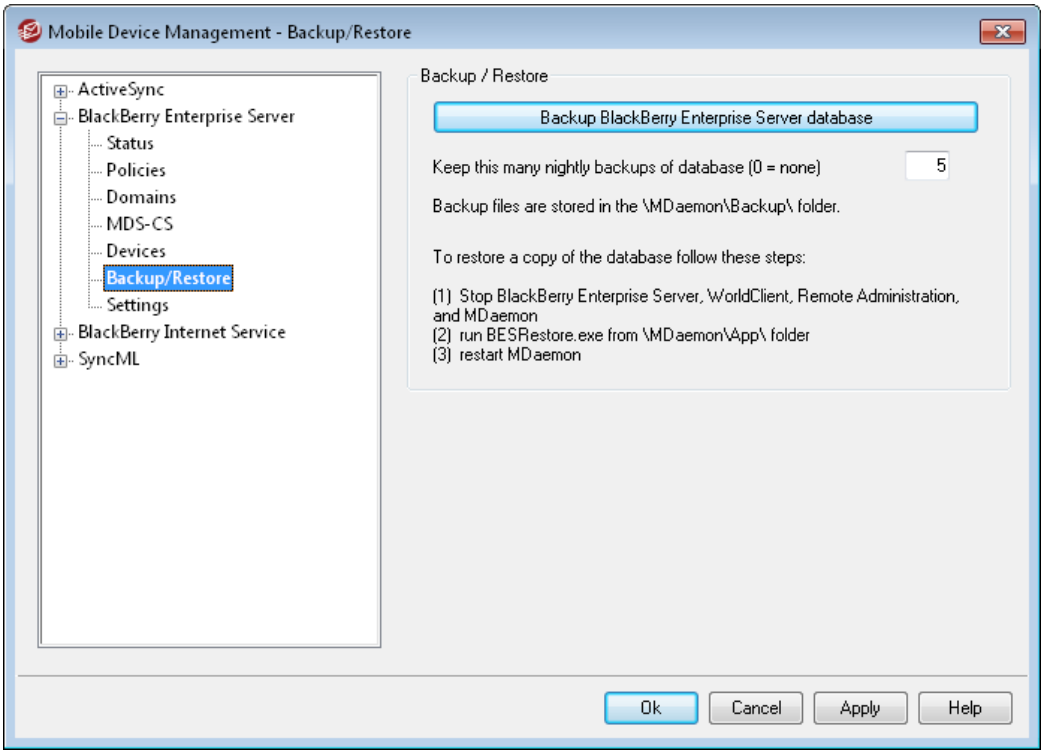
Start a slow sync for all BlackBerry activated accounts
Click this button to initiate a slow sync of all activated accounts. This resynchronizes all account data, ensuring that the data on the devices matches the data in MDaemon. Depending on the number of accounts and amount of data to be synchronized, this could take a long time to complete. Once started it will continue in the background until finished. You will be asked to confirm the decision to start a slow sync. There is an option located on the Account Editor's BlackBerry Enterprise Server 553 screen that can be used to initiate a slow sync for a specific account. See Settings 330 for more BlackBerry Enterprise Server synchronization options.

See:

BlackBerry Enterprise Server 314
Account Editor » BlackBerry Enterprise Server 553
BlackBerry Enterprise Server » Settings 330

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.8.2.6 Backup/Restore



Backing up the BlackBerry Enterprise Server database

Use the options on the Backup/Restore screen to backup your BlackBerry Enterprise Server database.

Backup BlackBerry Enterprise Server database files
Click this button if you wish to do an immediate, manual backup of your BlackBerry Enterprise Server database. The backup file is stored in the `\MDaemon\Backup\` folder. An entry about the backup's progress will appear on the System tab of MDaemon's Main Display 41.

Keep this many nightly backups of BlackBerry Enterprise Server database files (0=none)
Each night the BlackBerry Enterprise Server database is backed up and the backup files are stored in the `\MDaemon\Backup\` folder. This option determines the number of backup files that will be saved. When the limit is reached, the oldest file will be deleted when a new backup file is created. Use "0" in this option if you do not wish to do automatic nightly backups.

This value limits the number of backup files that will be saved, including manual backups initiated by clicking the *Backup BlackBerry Enterprise Server database files* button. If the value is set to "0" then no nightly backup will be performed, but you can still do manual backups, and there is no limit to the number of manual backup files that can be saved.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Restoring the BlackBerry Enterprise Server database

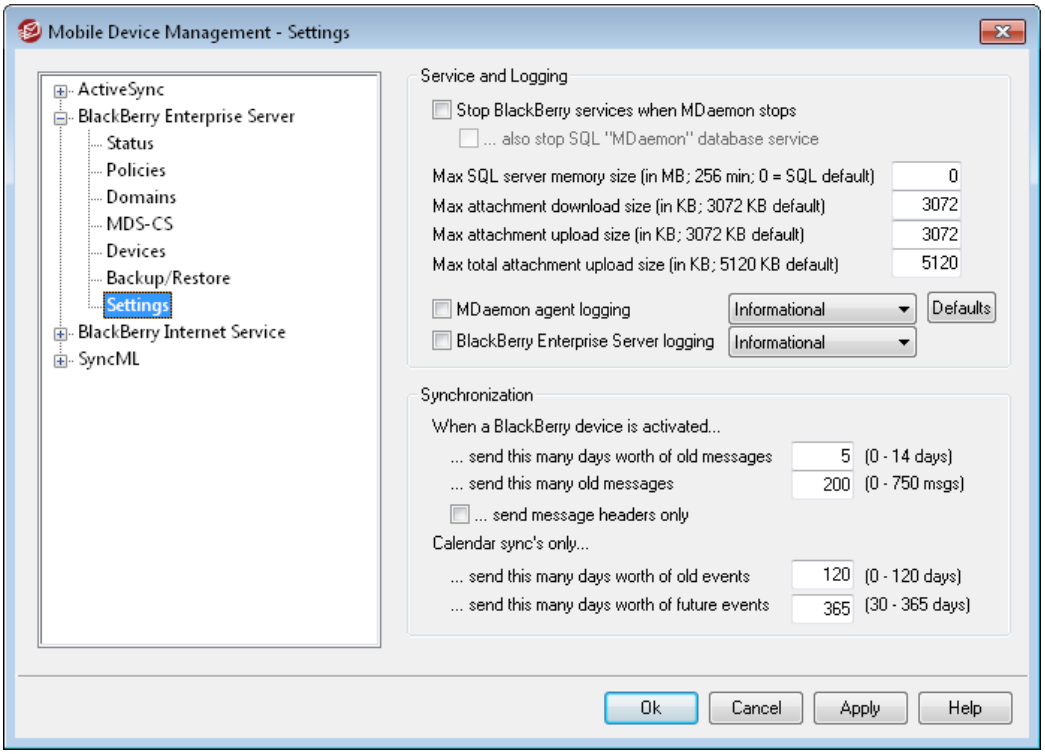
To restore your BlackBerry Enterprise Server database from a backup file:

1. Stop the BlackBerry Enterprise Server, WorldClient, Remote Administration, and finally MDaemon.
2. Run the MDaemon BlackBerry Enterprise Server Database Restore Utility (`BESRestore.exe`) in the `\MDaemon\App\` folder.
3. Click **Browse** and select the backup file.
4. Click **Open**.
5. Click **Restore Now**.
6. Restart MDaemon, Remote Administration, WorldClient, and the BlackBerry Enterprise Server.

See:

BlackBerry Enterprise Server 314
Account Editor » BlackBerry Enterprise Server 553

3.8.2.7 Settings


Mobile Device Management - Settings
ActiveSync
BlackBerry Enterprise Server
Status
Policies
Domains
MDS-CS
Devices
Backup/Restore
Settings
BlackBerry Internet Service
SyncML
Service and Logging
Stop BlackBerry services when MDaemon stops
... also stop SQL "MDaemon" database service
Max SQL server memory size (in MB; 256 min; 0 = SQL default) 0
Max attachment download size (in KB; 3072 KB default) 3072
Max attachment upload size (in KB; 3072 KB default) 3072
Max total attachment upload size (in KB; 5120 KB default) 5120
MDaemon agent logging
Informational
Defaults
BlackBerry Enterprise Server logging
Informational
Synchronization
When a BlackBerry device is activated...
... send this many days worth of old messages 5 (0 - 14 days)
... send this many old messages 200 (0 - 750 msgs)
... send message headers only
Calendar sync's only...
... send this many days worth of old events 120 (0 - 120 days)
... send this many days worth of future events 365 (30 - 365 days)
Ok
Cancel
Apply
Help

With this screen you can set the BlackBerry Enterprise Server services to stop when MDaemon stops, configure logging options, and set several synchronization options for

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

email and calendar data.

Service and Logging

Stop BlackBerry services when MDaemon stops
Check this box if you want the BlackBerry services 318 to stop whenever MDaemon stops.

...also stop SQL "MDaemon" database service
If you configure the BlackBerry services to stop when MDaemon stops, and you want the SQL "MDaemon" database service to stop also, then click this checkbox. Ordinarily the SQL "MDaemon" database service is left running, even if MDaemon or the BlackBerry services are stopped.

Max SQL server memory size (in MB; 256 min; 0=SQL default)
You can use this option to set a maximum memory size for the SQL server. This value is in MB and it must be set to at least "256". Use "0" in this option if you wish to use the SQL default setting.

Max attachment download size (in KB; 3072 KB default)
Use this option to specify the maximum size of attachments that can be downloaded to a BlackBerry device.

Max attachment upload size (in KB; 3072 KB default)
This option specifies the maximum size of each separate attachment that can be uploaded in an email from a BlackBerry device.

Max total attachment upload size (in KB; 5120 KB default)
This is the maximum combined size of attachments that can be uploaded together in an email message from a BlackBerry device.

Logging Settings

There are two BlackBerry logging options: **MDaemon agent logging** and **BlackBerry Enterprise Server component logging**. You can enable/disable them separately and set the level of logging detail that will be maintained for each. There are four levels of logging detail to choose from: *Error*, *Warning*, *Informational*, and *Debug*. *Error* is the lowest level of logging and *Debug* is the highest, which should generally be used only when diagnosing a problem. *Informational* maintains a good level of detail and is the default setting for both options. Click **Defaults** to restore the logging levels to the default settings.

Whenever you change the logging level the BlackBerry Enterprise Server services will be restarted.

The BlackBerry log files use MDaemon's global Logging 115 settings for size and roll-over but are slightly different in format than other MDaemon logs. The logs are stored in the `\Logs\BES\` subfolder.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Synchronization

When a device is activated...
These option are used to ensure that when a BlackBerry device is first activated, some of its old mail (mail sent or received prior to activation) will be synchronized with the device rather than only new mail. All mail processed for the account between the time it was enabled for BlackBerry device synchronization 553 and the device was activated will be synchronized with the device. If the number of messages or number of days worth of messages specified below have not been exceeded by the initial synch, then more mail will be synchronized according to the options.

...send this many days worth of old messages to the BlackBerry
Use this option to set the minimum number of days worth of old messages to send to the device when it is first activated. If it is set to 5, for example, then at least the last five days worth of messages will be sent.

This setting is also used during resynchronization (slow sync 328). Slow sync will only add messages missing from the database if they are more recent than the number of days specified here.

...send this many old messages to the BlackBerry
Use this option to set the number of old messages to synchronize with the device when it is first activated. This option takes precedence over the "*...send this many days worth of old messages*" option above, and the initial synchronization after activation may exceed this number of messages if more than that are processed between the time the account is enabled for BlackBerry device synchronization and when the device is activated. This option is set to **200** by default.

...send message headers only
Use this option to send only the message headers to the device rather than the entire message when old messages are synchronized.

Calendar syncs only...
These options determine the number of calendar events that will be synchronized with activated BlackBerry devices. Whenever these values are changed, a slow sync 328 must be performed in order for any events that would be affected by the change to be added or deleted from the devices. A calendar slow sync occurs automatically every night at midnight.

...send this many days worth of old events to the BlackBerry
This is the number of days worth of past calendar events that will be synchronized with the BlackBerry device calendar. Recurring events older than this number of days will still appear on the device calendar if one of the event's occurrences lies within the designated limit.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...send this many days worth of future events to the BlackBerry
This is the number of days worth of future events that will be synchronized with the BlackBerry device.

If there are any existing calendar entries on the device before it is activated, you must either wipe the device or reset the calendar. Otherwise existing calendar data on the MDaemon server may not be sent to the device. If you choose to reset the calendar rather than wipe the device, the reset may be performed after activation. See **Resetting the Device Calendar** below for more information. Always backup your device data before erasing it or resetting the calendar.

Resetting the Device Calendar

Overview (article KB15139)

Warning: The following procedures will delete all calendar data on the BlackBerry smartphone and re-synchronize the calendar back to the BlackBerry smartphone.

Note: Back up the data prior to performing the procedure. For instructions, see article KB12487.

Complete the steps for the version of BlackBerry Device Software installed on the BlackBerry smartphone.

BlackBerry Device Software version 4.2

On the BlackBerry smartphone, complete the following steps:

1. On the menu in the Calendar application, click **Options**.
2. Scroll to the bottom of the screen, and type **RSET**.

Note: For BlackBerry smartphones that support SureType® technology, use the multi-tap input method.

BlackBerry Device Software version 4.3 to 5.0

On the BlackBerry smartphone, complete the following steps:

1. On the menu in the Calendar application, click **Options**.
2. While the Options screen is displayed, type **RSET**.

Note: For BlackBerry smartphones that support SureType technology, use the multi-tap input method.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Additional Information

Wireless calendar synchronization process

Wireless calendar synchronization is turned on
If wireless synchronization of the calendar is turned **on**, the following message will appear:

This will erase your <nameofcalendar> calendar, and reload it from your server. Continue?

After the calendar data has been deleted, the following message will appear:

The <nameofcalendar> calendar has been wiped. It will be repopulated from your server.

The calendar will be repopulated with calendar data from the BlackBerry Enterprise Server.

Wireless calendar synchronization is turned off
If wireless synchronization of the calendar is turned **off**, the following message will appear:

Wireless Calendar, for <nameofcalendar>, is not enabled. Wipe Calendar anyway?

After the calendar data has been deleted, the following message will appear:

The <nameofcalendar> calendar has been wiped.

The calendar must then be repopulated with calendar data using BlackBerry Desktop Manager through a wired synchronization.

Re-population of calendar

During re-population of the calendar, the following message may appear on the BlackBerry smartphone:

Organizing Calendar

The performance of the BlackBerry smartphone may be affected during the re-population of the calendar. The speed of re-population depends on the amount of data transmitted and the speed of the wireless network.

See:

BlackBerry Enterprise Server 314
Account Editor » BlackBerry Enterprise Server 553

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.8.3 BlackBerry Internet Service

MDaemon is equipped with direct support for the BlackBerry Internet Service (BIS). BlackBerry Internet Service users can integrate their MDaemon mail account with their BlackBerry smartphone, allowing for BlackBerry push mail as well as improved email handling when using a BlackBerry device with MDaemon. Any BlackBerry device set up to pull mail from MDaemon via IMAP or POP prior to MDaemon version 11.0 can now be set up for push mail instead. Further, messages that are composed on the device will be sent to your MDaemon for delivery rather than having the BlackBerry Internet Service servers deliver them. This allows emails composed on a BlackBerry device to comply with your server's security policies, content-filter rules, DKIM, archiving, and so on.

Since the BlackBerry Internet Service only collects mail from a user's Inbox, this can cause problems for people who use IMAP Filters 541 to sort their messages to specific folders automatically. To overcome this problem, the BlackBerry Inbox 556 screen of the Account Editor and the Folders page in WorldClient allow the administrators and users, respectively, to choose which folders' new messages will be delivered to the user's device. When the BlackBerry Internet Service connects to MDaemon to collect new messages from the user's Inbox, MDaemon will also push the new messages from the selected folders. All new messages from all the selected folders will be sent to the BlackBerry device's Inbox. This does not push the actual folders to the device, it pushes only the new messages that they contain.

Finally, an internal folder aliasing scheme allows each user's "Sent Items" and "Deleted Items" folders to appear as values that the BlackBerry Internet Service recognizes, no matter what those folders are actually called in the user's account. This helps ensure that sent and deleted messages are placed into the proper MDaemon folders.

The BlackBerry Internet Service section of the BlackBerry dialog contains the following screens:

Domains 336 — use this screen to enable BlackBerry Internet Service integration for whichever domains you choose. There are options for entering the Subscribe URL and the SMTP server to which the BlackBerry Internet Service should pass messages when they are composed on a BlackBerry device. There is a history text box on the bottom of the screen that lists your BlackBerry Internet Service subscribe/unsubscribe activity, and there are several SSL and STARTTLS related options.

Subscribers 338 — this screen lists the subscription numbers of all MDaemon accounts that are setup for BlackBerry Internet Service push mail and are thus integrated directly with MDaemon. Even if an account is not listed as an integrated account, a BlackBerry Internet Service server may still be able to collect mail on behalf of the BlackBerry device via POP3 or IMAP, but it will not have the advantage of being able to send messages through your MDaemon server.

Settings 340 — this screen has several global options governing MDaemon's BlackBerry integration features. For example, you can choose whether or not to allow MDaemon to push mail from non-Inbox folders, you can choose to apply Attachment Linking 262 to Devices, you can allow multiple devices to integrate with a single MDaemon account, and several other options.

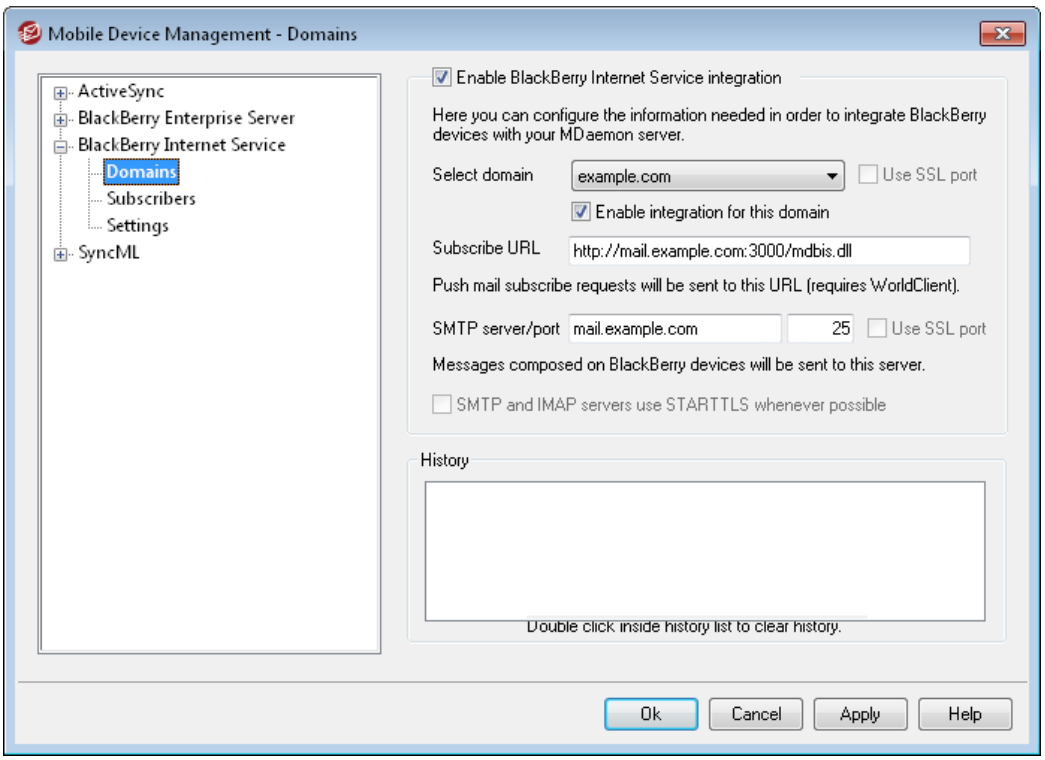
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

MDaemon requires all IMAP/POP sessions from BlackBerry Internet Service users to use a full email address when logging in to MDaemon. Thus when configuring their BlackBerry devices to collect mail they will need to use the full email address as the login parameter instead of just the mailbox portion of the address. This is necessary in order to avoid possible conflicts and to achieve proper account integration. This might mean that some of your existing users will have to delete and recreate the mail profile on their device, or at least change their login value to the full address.

See:

BlackBerry Internet Service » Domains 336
BlackBerry Internet Service » Subscribers 338
BlackBerry Internet Service » Settings 340
Account Editor » BlackBerry Internet Service 556

3.8.3.1 Domains



Enable BlackBerry Internet Service (BIS) integration

Check this box if you wish to enable MDaemon's BlackBerry Internet Service integration feature. You can then enable/disable it for individual domains by using

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

the options below.

When BlackBerry Internet Service integration is disabled globally or for particular domains, any accounts already subscribed to the BlackBerry Internet Service will continue to operate as before. No future BlackBerry devices will be integrated, but any existing integrations are unaffected.

Select domain
Select the domain in the drop-down list that you wish to configure for BlackBerry Internet Service integration. Any changes you make to the remaining settings will apply only to that domain.

Enable integration for this domain
Click this option to activate the BlackBerry Internet Service integration feature for the selected domain.

Use SSL port
If you have enabled SSL 489 in MDaemon, check this box if you want the BlackBerry Internet Service IMAP client to use the dedicated SSL port. The BlackBerry Internet Service IMAP client only supports SSL on the dedicated port.

Subscribe URL
This is the WorldClient URL to which the BlackBerry Internet Service will send subscribe and unsubscribe requests. When a user adds his MDaemon email account to his BlackBerry device, the BlackBerry Internet Service will send a subscribe request to this URL within approximately twenty minutes. MDaemon will then add the account to the Subscribers 338 screen. Subscription requests are managed by WorldClient, therefore WorldClient must be active.

When using IIS rather than WorldClient's native web server, you must add `MDbis.dll` (located in `MDaemon\Worldclient\HTML\`) to IIS in order for incoming SUBSCRIBE commands to be processed properly.

SMTP Server/port
This is the SMTP server and port to which all email composed on the integrated account's device will be sent for delivery.

Use SSL port
If you have enabled SSL 489 in MDaemon, check this box if you want the BlackBerry Internet Service SMTP client to use the dedicated SSL port.

The BlackBerry Internet Service SMTP client does not support SSL with self-signed certificates. Therefore if you wish to use SSL then you must use a commercial, third-party certificate.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

SMTP and IMAP servers use STARTTLS whenever possible
When MDaemon's STARTTLS 489 feature is enabled, check this box if you want the SMTP and IMAP servers to use STARTTLS whenever possible.

> The BlackBerry Internet Service does not support STARTTLS with self-signed certificates. Therefore if you wish to use STARTTLS then you must use a commercial, third-party certificate.

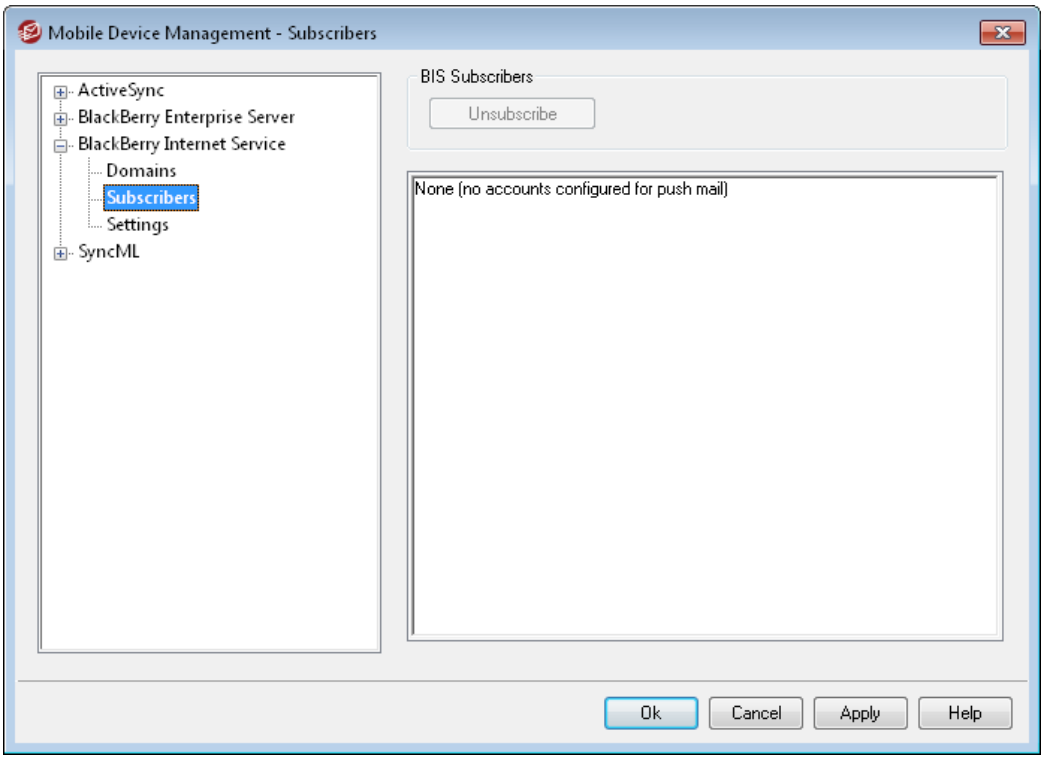
History

This box lists the BlackBerry Internet Service subscribe/unsubscribe history for your accounts. Each entry lists whether it was a subscribe or unsubscribe action, the email address, and the date and time of the activity.

See:

BlackBerry Internet Service 335
BlackBerry Internet Service » Subscribers 338
BlackBerry Internet Service » Settings 340
Account Editor » BlackBerry Internet Service 556

3.8.3.2 Subscribers



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Configuring Accounts to Push Mail to a BlackBerry Smartphone

The Subscribers screen lists all of your MDaemon accounts that are configured to push mail to a BlackBerry smartphone. To setup a new account for push mail:

1. Enable the BlackBerry Internet Service integration options for the server and domain on the Domains 336 screen, and make sure that the *Subscribe URL* and *SMTP server* value are pointing to WorldClient and your MDaemon server, respectively.
2. If the BlackBerry smartphone is already collecting mail from the user's MDaemon account, because the account was added to the device prior to activating MDaemon's BlackBerry Internet Service features, then delete that email account from the device. In the next step you will need to recreate the account on the device so that you can trigger push mail setup within the BlackBerry Internet Service.
3. Add the MDaemon email account to the user's BlackBerry smartphone, using the **full email address** and password as its login credentials. For detailed instructions on how to add an email account to a BlackBerry smartphone, see the device's online help or documentaion. You must only add the account in this step, not edit it. After creating the account, do not edit its signature, name settings, advanced options, or the like. You can make changes to the account later, in step 6.
4. Shortly after the account is added to the device, the *Subscribe URL* associated with the user's domain will receive a SUBSCRIBE request from the BlackBerry Internet Service service. This incoming request will be processed by WorldClient and the subscribed account will appear in the Subscribers list. The SUBSCRIBE request usually takes about 5 minutes to arrive, but can take up to 20.
5. Almost immediately after adding the account to the device it should receive an "*Email activation information*" email. Then, once the SUBSCRIBE request is properly received and processed, the BlackBerry device will receive a second email: "*Email activation information (push mail)*." Once that second email is received you know that the account has been successfully configured for push mail in MDaemon.
6. Make any desired changes to the email account on the device. You can add a signature, edit the name, adjust the advanced settings, and so on.

While waiting for the SUBSCRIBE request from the BlackBerry Internet Service to arrive, any changes to the email account on the device (such as signature text, advanced setup options, etc) will invalidate the request and you will not receive it. Therefore you must make no changes to the account on the device until the SUBSCRIBE request arrives. Otherwise you will need to delete the account and recreate it in order to restart the SUBSCRIBE process.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

This level of integration is not possible using POP. Any of your BlackBerry users currently using POP to collect mail will need to delete their email profile and recreate it using IMAP (not POP) which may require accessing advanced setup options on the BlackBerry. Consequently, MDaemon's IMAP server must be running for this feature to work.

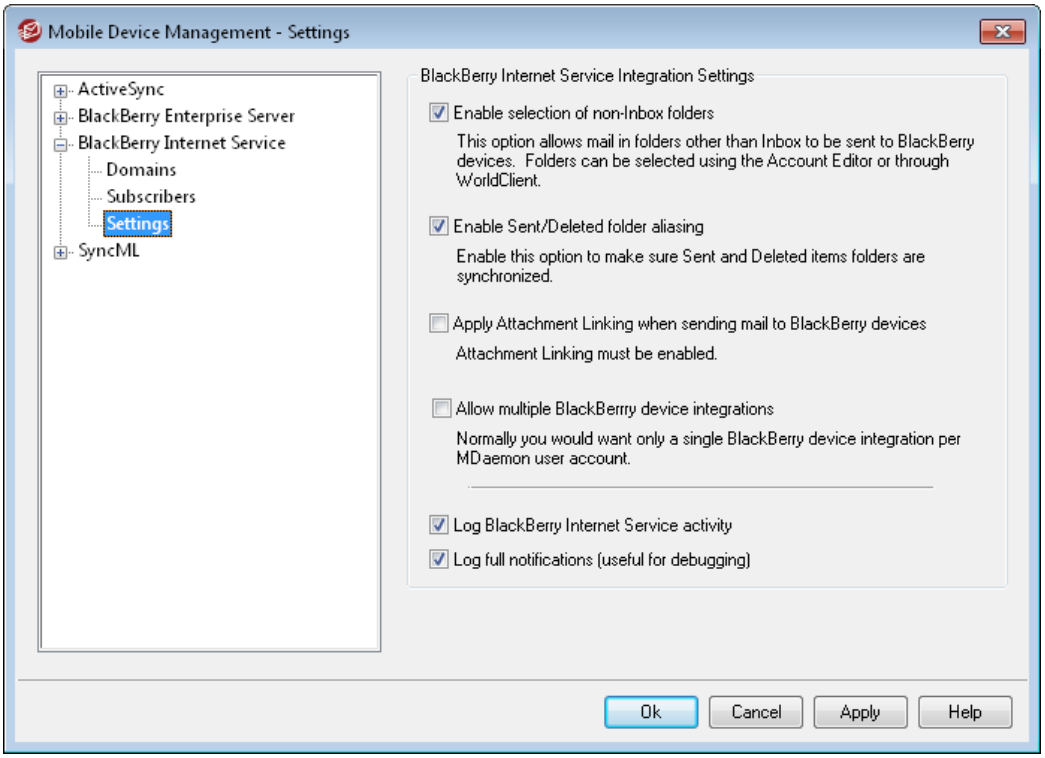
Unsubscribing an Integrated Account

Unsubscribing from push mail can be done by deleting the email profile using the BlackBerry device itself. The BlackBerry Internet Service will then send MDaemon an UNSUBSCRIBE request and the account will be unlinked. The UNSUBSCRIBE request may take some time to arrive and this poses no operational issues.

See:

BlackBerry Internet Service 335
BlackBerry Internet Service » Domains 336
BlackBerry Internet Service » Settings 340
Account Editor » BlackBerry Internet Service 556

3.8.3.3 Settings


Mobile Device Management - Settings
ActiveSync
BlackBerry Enterprise Server
BlackBerry Internet Service
Domains
Subscribers
Settings
SyncML
BlackBerry Internet Service Integration Settings
Enable selection of non-Inbox folders
This option allows mail in folders other than Inbox to be sent to BlackBerry devices. Folders can be selected using the Account Editor or through WorldClient.
Enable Sent/Deleted folder aliasing
Enable this option to make sure Sent and Deleted items folders are synchronized.
Apply Attachment Linking when sending mail to BlackBerry devices
Attachment Linking must be enabled.
Allow multiple BlackBerrry device integrations
Normally you would want only a single BlackBerry device integration per MDaemon user account.
Log BlackBerry Internet Service activity
Log full notifications (useful for debugging)
Ok
Cancel
Apply
Help

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

BlackBerry Internet Service Integration Settings

Enable selection of non-Inbox folders
By default in MDaemon, messages placed in non-Inbox IMAP folders can be pushed to a BlackBerry smartphone's Inbox. This is managed through the BlackBerry Inbox 556 screen of the Account Editor and the Folders page in WorldClient. These screens allow the administrators and users, respectively, to choose which folders' new messages will be delivered to the user's device. If you do not wish to allow users with a BlackBerry device to collect mail from any of their IMAP folders other than the Inbox, then disable this option. However, we recommend that you leave this option enabled, because if you disable it then those who use IMAP Filters 541 to sort their messages into specific folders will not be able to get those filtered messages on their device.

This feature operates independently from the account integration options on the Domains 336 and Subscribers 338 screens. Even if you disable BlackBerry Internet Service integration in MDaemon, a user can still create an email account on his BlackBerry device to collect his mail from MDaemon, just as he can collect it using any other traditional email client or smartphone. This feature simply makes it possible for BlackBerry smartphone users to collect messages from the folders that they are using IMAP filters to manage.

Enable Sent/Deleted folder aliasing
By default an internal folder aliasing scheme allows each user's "Sent Items" and "Deleted Items" folders to appear as values that the BlackBerry Internet Service recognizes, no matter what those folders are actually called in the user's account. This doesn't alter any folder names in any way. It is entirely an internal aliasing function to help ensure that sent and deleted messages are placed into the proper MDaemon folders. As with the above option, this option operates independently from the account integration options. It can be used even if the *Enable BlackBerry Internet Service integration* option is disabled on the Domains screen. If you do not wish to alias these folders for BlackBerry users, disable this option.

Users can designate the folders they wish to use as their Sent Items and Deleted Items folders from the Folders page in WorldClient.

Apply Attachment Linking when sending mail to BlackBerry devices
Check this box if you wish to apply the Attachment Linking 262 feature to all messages sent to BlackBerry Subscribers 338. The *Enable attachment linking* feature on the Attachment Linking dialog must be enabled for this to work.

Allow multiple BlackBerry device integrations
Enable this option if you wish to allow multiple BlackBerry devices to integrate with the same MDaemon account. This means, for example, that someone with two BlackBerry smartphones could set up both devices to get push mail from the user's

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

single account.

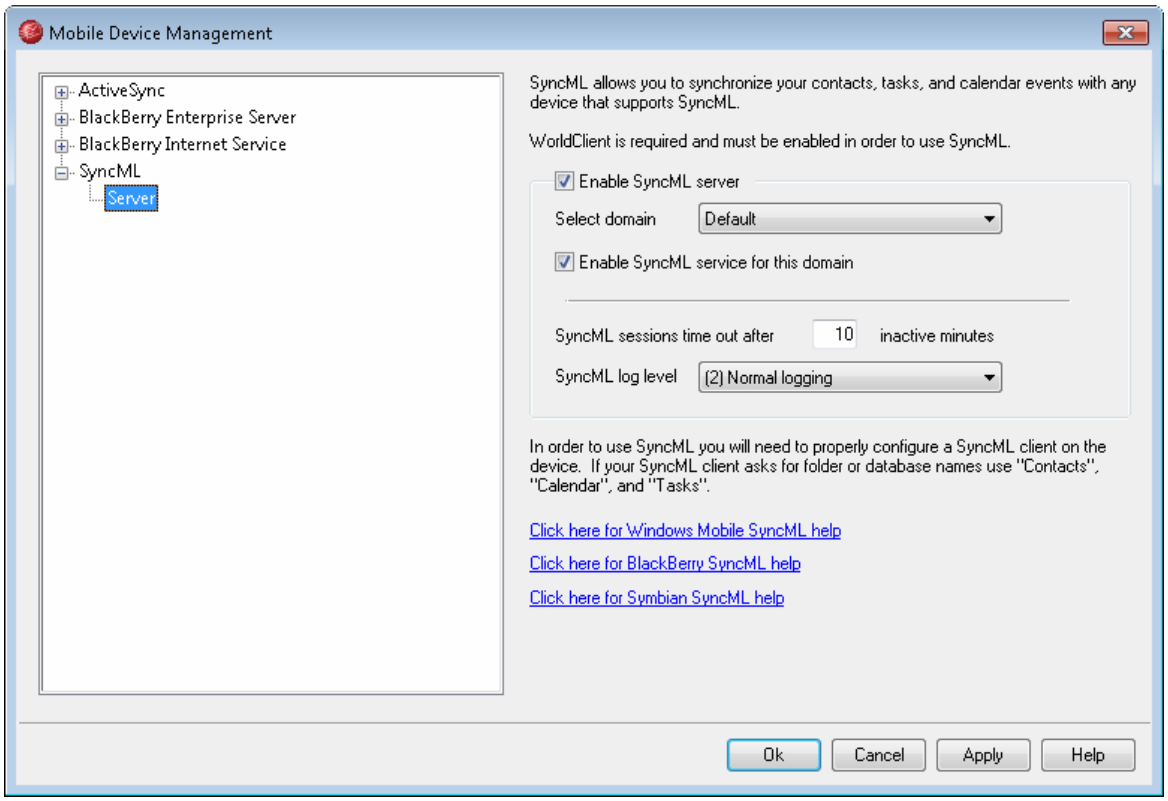
Log BlackBerry Internet Service activity)
Check this box if you wish to log the BlackBerry Internet Service activity. It will be copied to the log files and appear on the BIS tab of the main GUI.

Log full notifications (useful for debugging)
Check this box if you wish to log all activity from BlackBerry Internet Service servers. This option can be useful for debugging, to help you diagnose BlackBerry Internet Service related problems.

See:

BlackBerry Internet Service 335
BlackBerry Internet Service » Domains 336
BlackBerry Internet Service » Subscribers 338
Account Editor » BlackBerry Internet Service 556

3.8.4 SyncML


Mobile Device Management
ActiveSync
BlackBerry Enterprise Server
BlackBerry Internet Service
SyncML
Server
SyncML allows you to synchronize your contacts, tasks, and calendar events with any device that supports SyncML.
WorldClient is required and must be enabled in order to use SyncML.
Enable SyncML server
Select domain
Default
Enable SyncML service for this domain
SyncML sessions time out after
10
inactive minutes
SyncML log level
(2) Normal logging
In order to use SyncML you will need to properly configure a SyncML client on the device. If your SyncML client asks for folder or database names use "Contacts", "Calendar", and "Tasks".
Click here for Windows Mobile SyncML help
Click here for BlackBerry SyncML help
Click here for Symbian SyncML help
Ok
Cancel
Apply
Help

WorldClient includes a SyncML server that can be used to synchronize your Contacts, Tasks, and Calendar events with any SyncML capable mobile devices. If your BlackBerry smartphone or other device doesn't have built-in SyncML support then you must install a third-party synchronization client on it. Some example clients are:

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Funambol Sync Client, Synthesis, and SyncJE. There are also sync clients available for synchronizing your calendar with an email client such as Microsoft Outlook. The Funambol Sync Client, for example, is available for Outlook, BlackBerry, Windows Mobile, and other types of applications and devices. Several clients are available free of charge.

For more information on SyncML and the SyncML specification, visit the Open Mobile Alliance (OMA).

SyncML

Select domain
Use this drop-down list box to choose the domain you wish to configure. After selecting the domain, check or uncheck the "*Enable SyncML server*" box and then click Apply or OK to save the setting. Choose "Default" from the drop-down list to designate the default setting. The default setting will be applied to all new domains and all existing domain for which you have not specifically defined a SyncML setting.

Enable SyncML server
Enable or disable this option to designate whether or not the SyncML server will be accessible by the domain selected in the *Select domain* option above.

SyncML sessions time out after XX inactive minutes
This is the length of time a SyncML session will be permitted to remain inactive before it will time out and be closed. This is a global setting—it applies to all SyncML sessions regardless of the domain.

SyncML log level
Use this drop-down list to designate the degree to which SyncML activities will be logged. There are six possible levels of logging: 1-Debug logging, 2-Normal logging, 3-Warnings and errors only, 4-Errors only, 5-Critical errors only, and 6-No logging. This is a global setting—it cannot be applied to specific domains.

3.8.4.1 Configuring Your SyncML Clients

In order to access WorldClient's SyncML server, your SyncML clients must be configured to connect to:

```
http://<WorldClient Server><:port>/MDSyncML.dll
```

Examples:

```
http://mail.example.com:3000/MDSyncML.dll
http://www.example.com/MDSyncML.dll
```

If your SyncML client asks for folder names, use `Contacts`, `Calendar`, and `Tasks`. Those names always expand to the user's default WorldClient folders of the corresponding type.

The SyncML server supports any of the following formats for the folder paths:

```
contacts
/contacts
./contacts
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

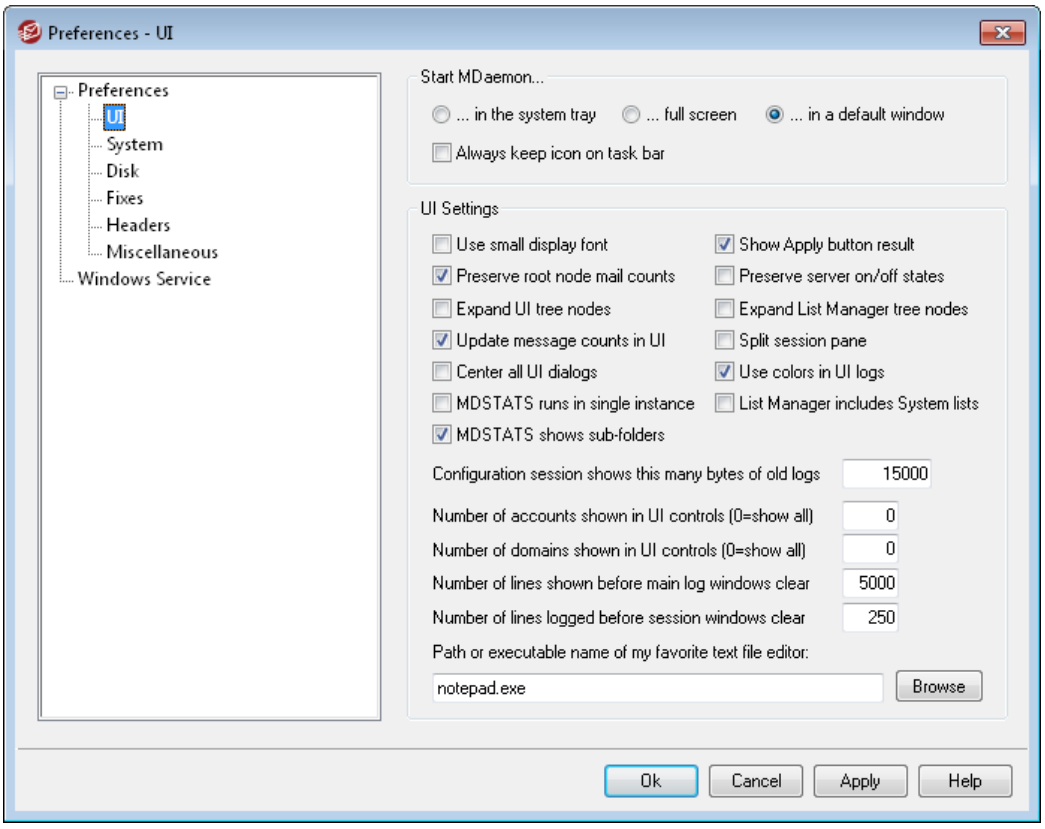
`contacts/phone` (assuming a phone sub-folder exists)
`contacts.imap\phone.imap`

Before attempting to synchronize using SyncML, a user must log in to WorldClient one time.

3.9 Preferences

3.9.1 Preferences

3.9.1.1 UI



Start MDaemon...

...in the system tray
Choose this option if you do not wish to display MDaemon's interface at startup. The MDaemon icon will still appear in the system tray.

...full screen
Choose this option if you want MDaemon's interface to be maximized at startup.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...in a default window
Choose this option if you want MDaemon's interface to appear in a default window at startup.

Always keep icon on task bar
When this option is enabled, MDaemon will start minimized to the taskbar, and it will appear on both the taskbar and in the system tray when minimized. Clear this checkbox if you do not want MDaemon to appear on the Windows taskbar when minimized; only the tray icon will be visible.

UI Settings

Use small display font
Enables the small display font in the Event Tracking and Session windows.

Show Apply button result
By default, whenever you click the Apply button on a dialog a message box will open confirming that the changes you made to the dialog's settings have been saved. Uncheck this box if you wish to apply the changes without displaying the message.

Preserve root node mail counts
Enable this option if you wish to save the root node counters across server reboots. The root node counters are listed in the "Statistics" section of the Stats pane on MDaemon's main GUI.

Preserve server on/off states
If this control is enabled, MDaemon will ensure that the state of its servers (enabled or disabled) remains the same after a reboot.

Expand UI tree nodes
Click this box if you want the navigation tree nodes in the left-hand pane of various dialog to be expanded automatically. This does not apply to the Mailing List Manager 180. If you wish to automatically expand the mailing list tree nodes, use the *Expand List Manager tree nodes* option below.

Expand List Manager tree nodes
Click this checkbox if you want the Mailing List Manager's 180 navigation tree nodes in the left-hand pane to be expanded automatically.

Update message counts in UI
This option governs whether MDaemon will check the disk to count waiting messages in the mail queues.

Split session pane
Enable this option if you want the Sessions tab in the main MDaemon UI to be split from the other tabs into its own pane. Changing this setting requires a restart of the MDaemon UI, and the option on the Windows menu to switch panes will no longer be available.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Center all UI dialog
Enable this option if you want dialogs to be centered on the screen when they are opened, rather than overlap each other. This is disabled by default.

Use colors in UI logs
This option will colorize the text displayed on several of the Event Tracking and Logging 41 tabs on MDaemon's user interface. It is enabled by default, and changing its setting will require an MDaemon interface restart before the change will take effect. See: Colorized Session Logs 119 for more information.

List Manager includes System lists
Enable this option if you wish to display MDaemon's system-generated mailing lists (e.g. Everyone@ and MasterEveryone@) in the Mailing List Manager 180. System generated lists have limited items available for user configuration. When this option is disabled, system lists will be hidden but still available for use. This option is disabled by default.

MDSTATS runs in single instance
Click this checkbox if you do not want more than one copy of MDaemon's Queue and Statistics manager 664 to be able to run at once. Attempting to launch the manager when it is already running will simply cause the currently running instance to become the active window.

MDSTATS shows subfolders
Click this checkbox if you want the Queue and Statistics manager 664 to display subfolders contained in the various queues and user mail folders.

Configuration session shows this many bytes of old logs
When running a configuration session, this is the maximum amount of log data that will be displayed on an Event Tracking and Logging 41 tab. The default setting is 15000 bytes.

Number of accounts shown in UI controls (0=show all)
This is the maximum number of accounts that will be shown in the drop-down list boxes on various dialogs. Further, when the value in this option is set lower than the number of accounts that currently exist, the "Edit Account" and "Delete Account" options will no longer appear on the Accounts menu; you will only be able to edit and delete accounts by using the Account Manager 518. You must restart MDaemon before any changes to this option will take effect. The default setting is "0", which causes all accounts to be shown.

Number of domains shown in UI controls (0=show all)
This is the maximum number of domains that will be displayed on the main GUI, regardless of how many domains actually exist. After changing this value you must restart MDaemon before the changes will be visible. The default setting is "0", which causes all domains to be shown.

Number of lines shown before main log windows clear
This is the maximum number of lines that will be displayed in the logging windows of the main display. When this number of lines is reached the window will be cleared.

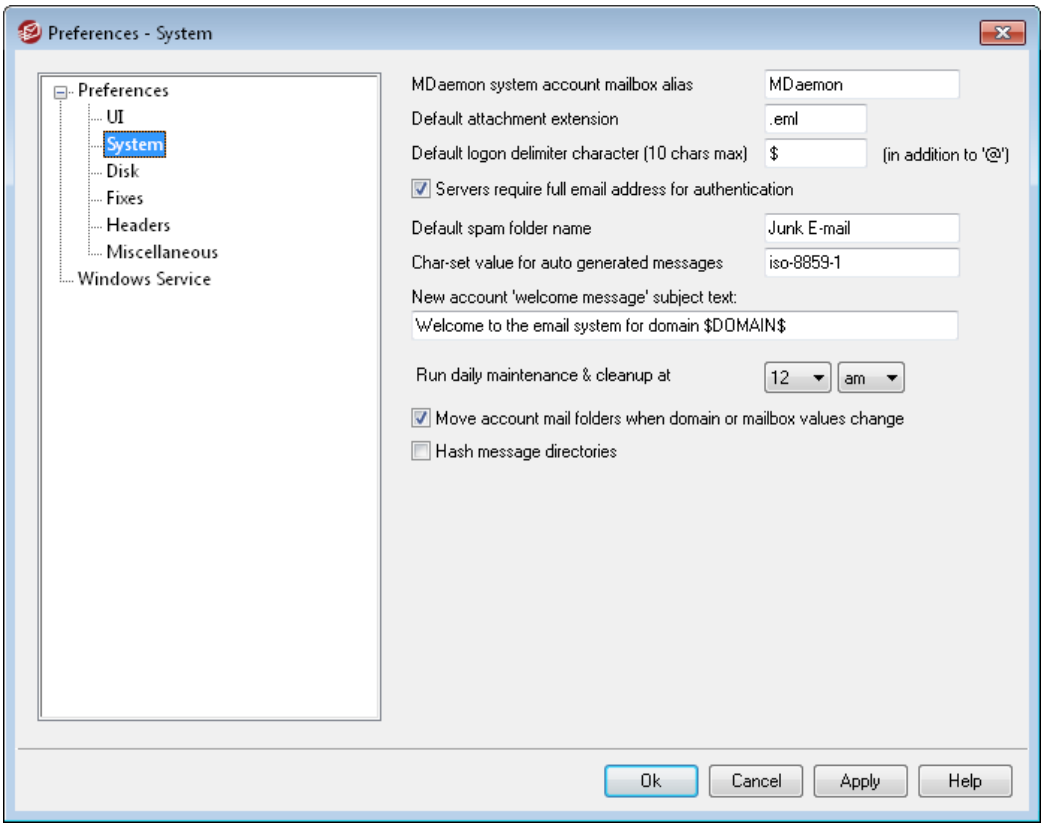
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

This has no affect on the log file; only the display will be cleared.

Number of lines logged before session windows clear
This is the maximum number of lines that will appear in each Session Window 46 before it is cleared. This has no affect on the log file.

Path or executable name of my favorite text file editor
Notepad.exe is the general text editor that the MDaemon UI will launch by default when needed. If you prefer to use a different text editor, enter its file path or executable name here.

3.9.1.2 System



MDaemon system account mailbox alias [address]
This is the email address from which system generated messages will come. Subscription confirmations, delivery status notification (DSN) messages, various other notification messages, and the like are all system messages.

Default attachment extension
System generated messages will be created using this extension. This will also be the extension assigned to attachments included with system generated messages. For example, if MDaemon generates a warning message to the postmaster about a specific message it will attach that message with this value as the file extension.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Default logon delimiter character (10 characters max)
When using an email address as the account logon parameter, this character or string of characters can be used as an alternative to "@". This may be necessary for some users that have email clients which do not support "@" in the logon field. For example, if you used "$" in this field then users could login using "user1@example.com" or "user1$example.com".

Servers require full email address for authentication
MDaemon's POP and IMAP servers require you to use your full email address by default when logging in to MDaemon. If you wish to allow mailbox only logins (e.g. "user1" instead of "user1@example.com") then you can disable this option, but it is not recommended as mailbox only logins are ambiguous when MDaemon is serving multiple domains.

Default spam folder name
Use this text box to specify the default name for the Spam folder that MDaemon can create automatically for your users. The default name is "Junk E-mail" to match the default value of various other widely distributed products.

Char-set value for auto-generated messages
Specify the character set that you wish to be used for auto-generated messages. The default setting is iso-8859-1.

New account "welcome message" subject text:
MDaemon typically sends a "welcome message" to new accounts. The text specified here will appear as the message's "Subject" header. The welcome message is constructed from the `NEWUSERHELP.DAT` file contained in the `…\MDaemon\app\` folder, and this subject header may contain any macros permitted in auto response scripts 621.

Run daily maintenance and cleanup at [1-12] [am/pm]
Use this option to set the hour at which the daily maintenance and cleanup event takes place. The default and recommended setting is 12am.

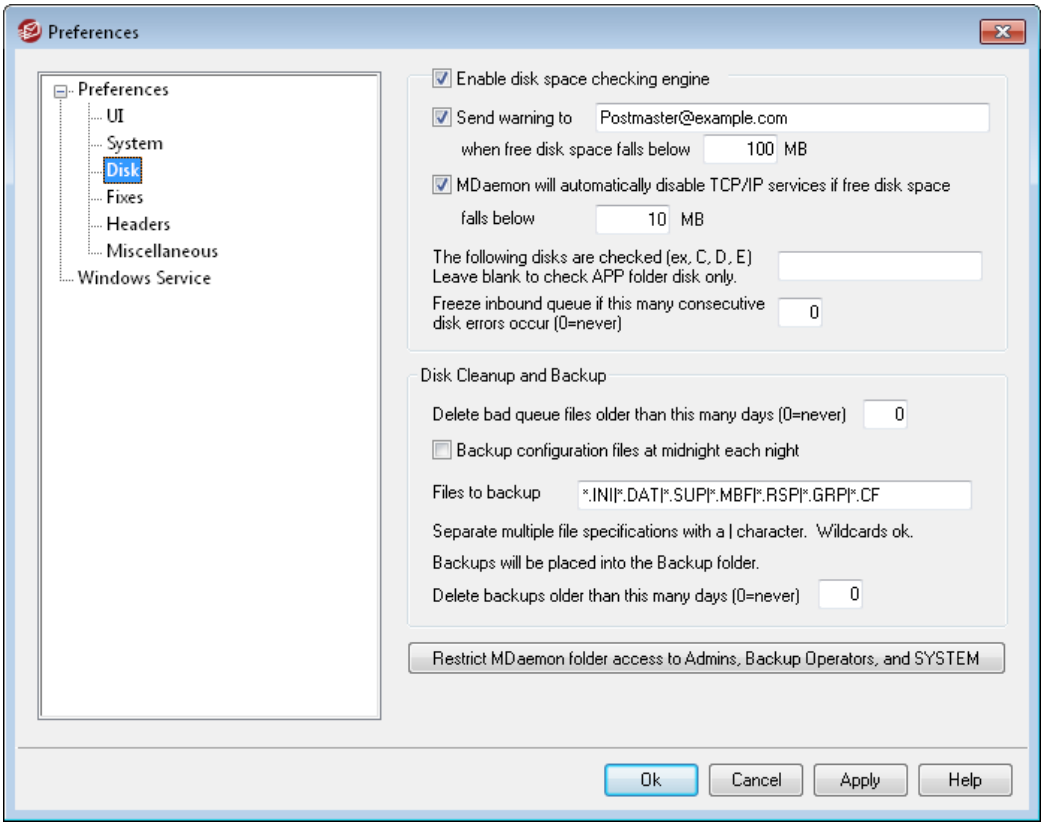
Regardless of the hour you set for this option, there are some daily events that will always happen at midnight, such as log file maintenance and running `midnight.bat`.

Move account mail folders when domain or mailbox values change
If this checkbox is enabled, when you change a domain name or mailbox the mail folders for the affected accounts will be moved to the new location. Otherwise, MDaemon will continue to use the old mail folder names.

Hash message directories
Click this check box if you wish to enable directory hashing — MDaemon will hash certain directories by making up to 65 sub-directories. Hashing can increase performance for certain hi-volume sites but may degrade performance slightly for typical MDaemon sites. This option is disabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.9.1.3 Disk



Enable disk space checking engine
Activate this checkbox if you want MDaemon to monitor the amount of disk space that is available on the drive where the `MDaemon.exe` is located.

Send warning to [user or address] when free disk space falls below [xx] MB
By using this option you can configure MDaemon to send a notification message to the user or address of your choice when disk space drops below a certain level. The default value is 100 MB.

MDaemon will automatically disable TCP/IP services if free disk space falls below [xx] MB
Enable this feature if you want MDaemon to disable TCP/IP Services if free disk space drops to a certain level. The default value is 10 MB.

The following disks are checked (ex: C, D, E)
Use this option if you wish to monitor the available disk space on multiple disks, specifying the drive letter for each one. If you leave it blank then only the disk that contains MDaemon's `\app\` folder will be checked.

Freeze inbound queue if this many consecutive disk errors occur (0=never)
If this number of disk errors occurs when processing the inbound queue, MDaemon will stop processing the queue until you resolve the situation. An email is placed in the postmaster's mailbox when this shut down occurs.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Disk cleanup and backup

Delete bad queue files older than this many days (0=never)
Use this option if you want MDaemon to delete old files from the bad message queue whenever they are older than the specified number of days. If you do not wish to delete messages automatically, use "0" in this option.

Backup configuration files at midnight each night
Click this checkbox if you want to archive all MDaemon configuration files at midnight each night to the Backups directory.

Files to backup
Use this text box to specify exactly which files and file extensions to back up. Wildcards are permitted and each filename or extension must be separated be the "|" character.

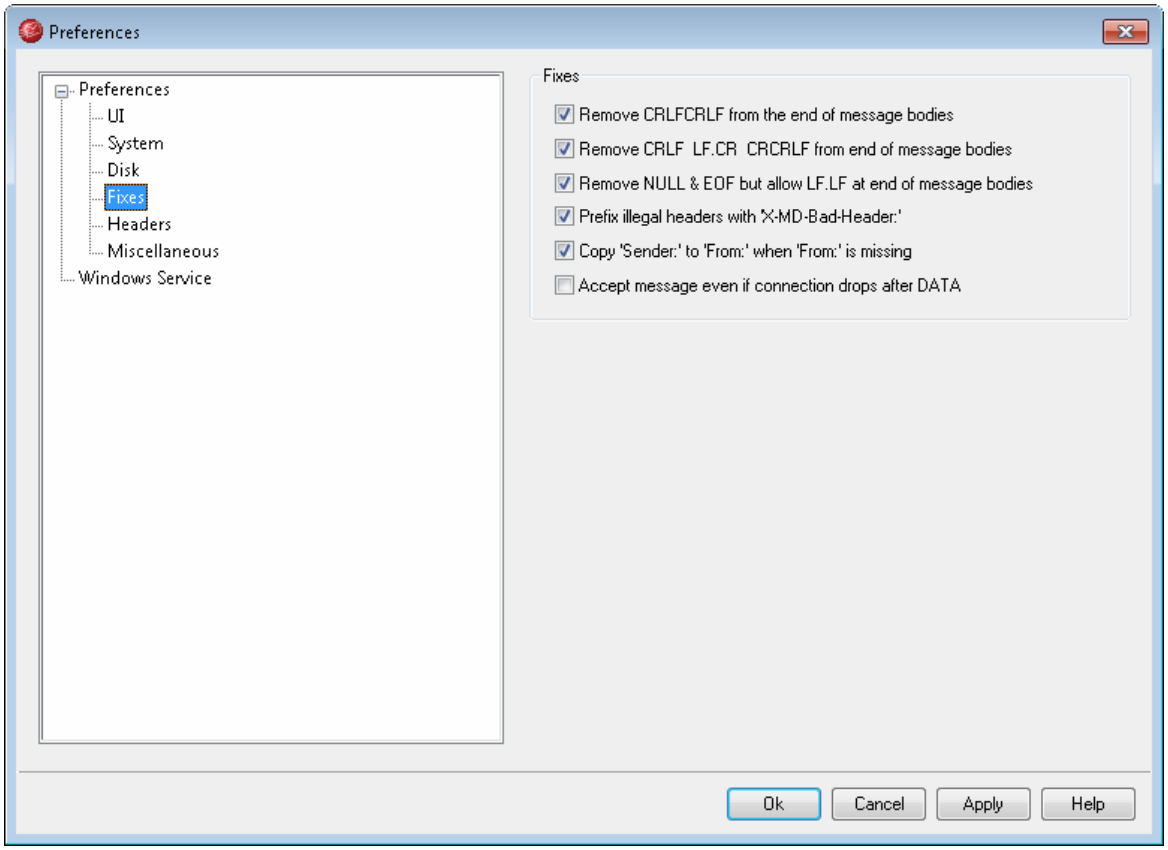
Delete backups older than this many days (0=never)
Use this option if you wish to delete old backup files automatically. Files older than the specified number of days will be deleted as part of the daily midnight cleanup event. The default setting is "0", which means that old backup files will not be deleted.

Restrict MDaemon folder access to Admins, Backup Operators, and SYSTEM

Click this button to restrict access to the `\MDaemon\` root folder and its subfolders to the following Windows accounts/groups: Administrators, Backup Operators, and SYSTEM.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.9.1.4 Fixes



Remove CRLFCRLF from the end of message bodies
Certain mail clients have problems displaying messages that end with consecutive Carriage Return Line Feeds (i.e. CRLFCRLF). When this box is checked, MDaemon will strip consecutive `CRLFCRLF` sequences from the end of the message body. This option is enabled by default.

Remove CRLF LF.CR CRCRLF from the end of message bodies
By default, MDaemon will remove this sequence from the end of messages, as it can cause problems for some mail clients. Uncheck this box if you do not wish to remove this sequence from messages.

Remove NULL & EOF but allow LF.LF at the end of message bodies
When this box is checked MDaemon will remove `Null` and EOF characters from the end of message bodies, but it will allow messages ending in `LF.LF`, as well as messages ending with the normal `CRLF.CRLF` sequence that signifies the end of a message. This option is enabled by default.

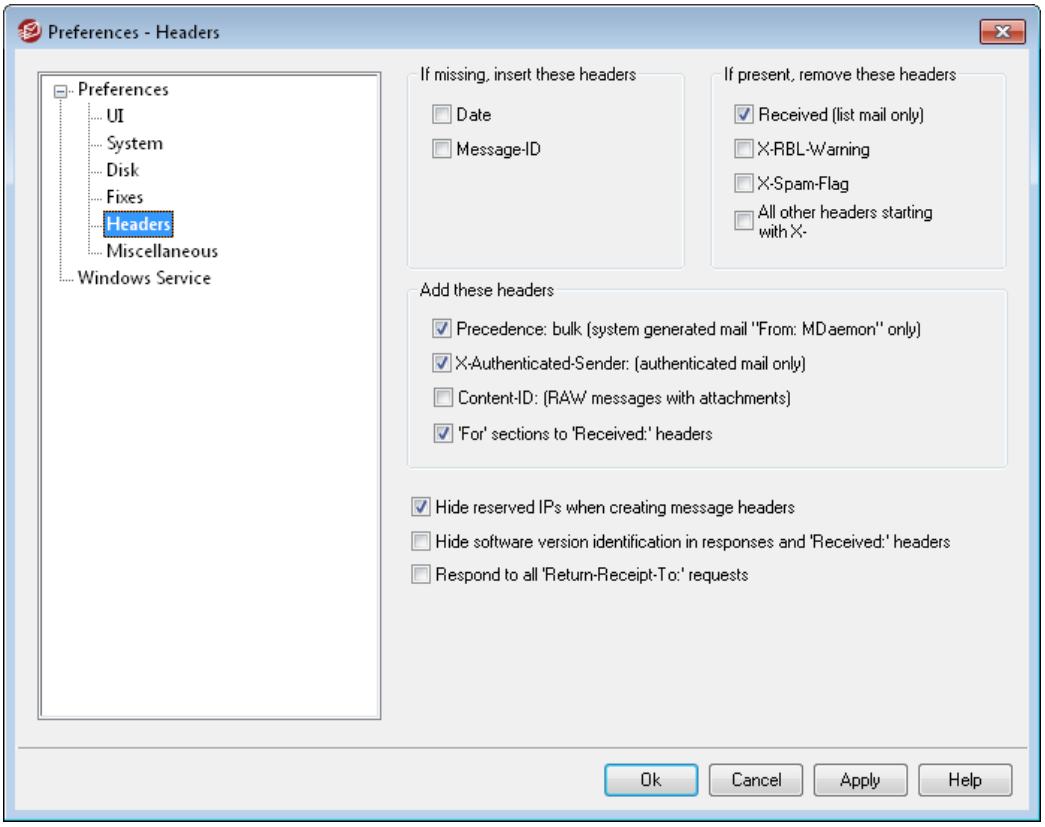
Prefix illegal headers with "X-MD-Bad-Header:"
When this option is enabled and MDaemon encounters a bad message header, it will prefix the bad header with "`X-MD-Bad-Header:`" This option is enabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Copy 'Sender:' to 'From:' when 'From:' is missing
Some mail clients fail to create a `FROM:` header when you compose a message. Instead, the `FROM:` header's information is placed in the `Sender:` header. This can cause problems for some mail servers as well as the recipient of your message. To help prevent these problems, MDaemon will create the missing `FROM:` header by using the contents of the `Sender:` header when this box is checked. This option is enabled by default.

Accept message even if connection drops after DATA
When this option is enabled, MDaemon will accept and deliver a message even if there's a connection abort during or immediately after the `DATA` command during the SMTP process. This should not be used under normal circumstances as it can lead to duplicate messages.

3.9.1.5 Headers



If missing, insert these headers

Date
When a message is encountered that doesn't have a "`Date:`" header, MDaemon will create one and add it to the message file if this option is enabled. It will be the date on which MDaemon first receives the message, not when it was created by the sender. There are some mail clients that do not create this header, and since some

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

mail servers refuse to honor such messages, this feature will enable them to be delivered.

Message-ID
When a message is encountered that doesn't have a "Message-ID" header, MDaemon will create one and insert it into the message.

If present, remove these headers

Received (list mail only)
Check this box if you wish to strip all existing "Received:" headers from mailing list messages.

X-RBL-Warning
Click this checkbox if you wish to strip out all "X-RBL-Warning:" headers found in messages. This option is disabled by default.

X-Spam-Flag
Enable this option if you wish to strip old "X-Spam-Flag:" headers from messages.

All other headers starting with X-
MDaemon and other mail servers use many server specific headers called X-Type headers in order to route mail and perform various other functions. When this option is enabled, MDaemon will strip these headers from messages. **Note:** this option does not remove X-RBL-Warning headers. If you wish to remove those headers, use the "*X-RBL-Warning*" option above.

Add these headers

Precedence: bulk (system generated mail 'From: MDaemon' only)
When this box is checked all system generated messages from MDaemon (welcome messages, warnings, "could not deliver" messages, and so on) will have a "Precedence: bulk" header inserted.

X-Authenticated-Sender: (authenticated mail only)
By default MDaemon will add the "X-Authenticated-Sender:" header to messages that arrive on an authenticated session using the AUTH command. Uncheck this box if you do not wish to add this header.

Content-ID: (RAW messages with attachments)
Check this box if you wish to add unique MIME Content-ID headers to messages that MDaemon creates from a RAW file that contains attachments.

'For' sections to 'Received:' headers
Click this switch if you want "For [SMTP Recipient]" sections to be added to the message's "Received:" header added by MDaemon.

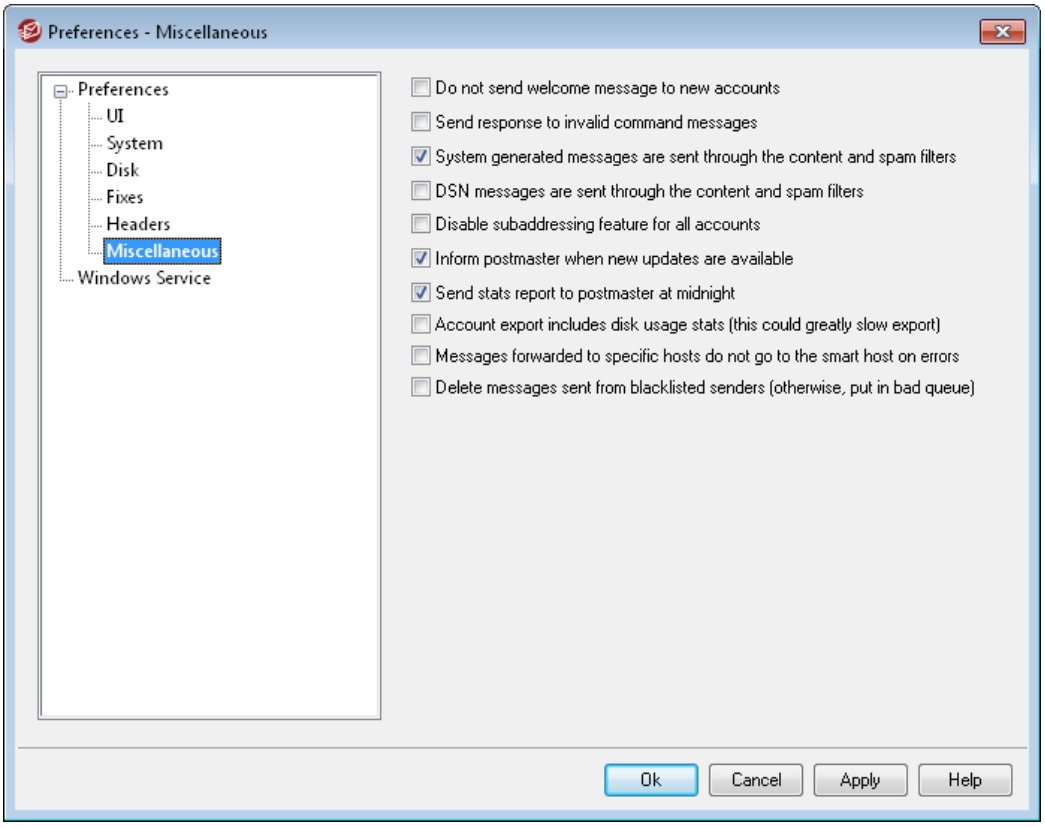
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Hide reserved IPs when creating message headers
This option is enabled by default and prevents reserved IP addresses from appearing in certain MDaemon created message headers. Reserved IP addresses include: `127.0.0.*`, `192.168.*.*`, `10.*.*.*`, and `172.16.0.0/12`. If you also wish to hide your domain IPs (including LAN domains) from the headers then you can set the following switch in MDaemon's `app\MDaemon.ini` file manually: `[Special] HideMyIPs=Yes` (default is `No`).

Hide software version identification in responses and 'Received:' headers
Use this option if you wish to prevent MDaemon from stating its software version and other identifying information when creating `Received` headers or responding to various protocol requests. This option is disabled by default.

Respond to all 'Return-Receipt-To:' requests
Click this check box if you wish to honor requests for delivery confirmation from incoming messages and automatically send a confirmation message to the sender. This option is disabled by default.

3.9.1.6 Miscellaneous


Preferences - Miscellaneous
Preferences
UI
System
Disk
Fixes
Headers
Miscellaneous
Windows Service
Do not send welcome message to new accounts
Send response to invalid command messages
System generated messages are sent through the content and spam filters
DSN messages are sent through the content and spam filters
Disable subaddressing feature for all accounts
Inform postmaster when new updates are available
Send stats report to postmaster at midnight
Account export includes disk usage stats (this could greatly slow export)
Messages forwarded to specific hosts do not go to the smart host on errors
Delete messages sent from blacklisted senders (otherwise, put in bad queue)
Ok
Cancel
Apply
Help

Do not send welcome message to new accounts
By default, MDaemon will generate a Welcome message based upon the `NEWUSERHELP.DAT` file and distribute it to new users when their account is created.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Enable this control if you want to prevent the message from being generated.

Send response to invalid command messages
By default when someone sends an email to the system account that does not contain a valid command, MDaemon does not respond with a "No valid command found" email. Enable this option if you wish to send a response to those emails.

System generated messages are sent through the content and spam filters
By default, system generated messages are processed through the Content Filter and Spam Filter. Clear this checkbox if you want them to be excluded from content and spam filtering.

DSN messages are sent through the content and spam filters
Enable this option if you wish to send DSN messages 661 through the content and spam filters. This option is disabled by default.

Disable subaddressing feature for all accounts
Click this option if you wish to globally disable the Subaddressing feature. Subaddressing will not be permitted for any account, regardless of the individual account settings. For more on Subaddressing, see the IMAP Filters 541 screen of the Account Editor.

Inform postmaster when new MDaemon updates are available
This option causes MDaemon to notify the postmaster whenever there is an MDaemon update available. This is enabled by default.

Send stats report to postmaster at midnight
By default a statistics report will be sent to the postmaster each night at midnight. Clear this checkbox if you do not want the report to be sent. This option corresponds to the Statistics 41 tab located on MDaemon's main display.

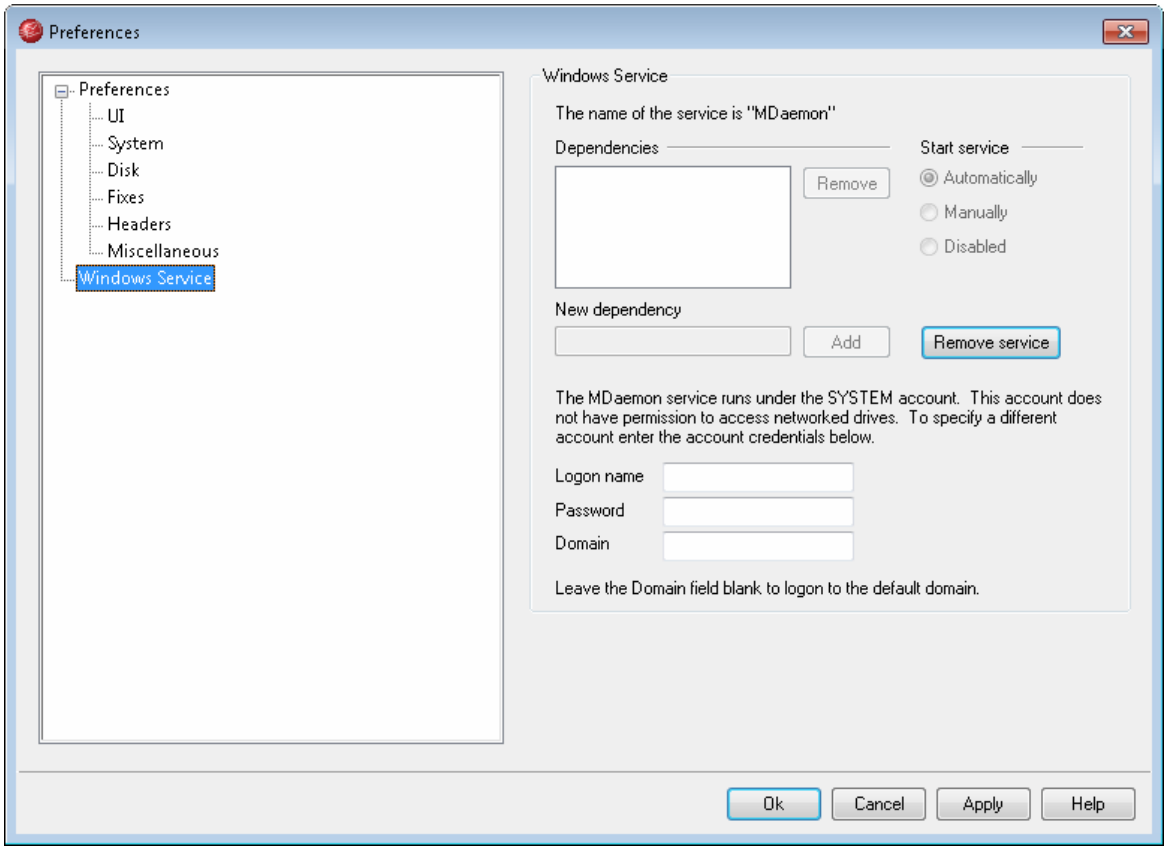
Account export includes disk usage stats (this could greatly slow export)
By default, account exports do not include disk file counts and space consumed. If you wish to include this information in exports, enable this checkbox. This may, however, significantly slow export speeds.

Messages forwarded to specific hosts do not go to the smart hosts on errors
Using the "Advanced Forwarding Settings" on the Account Editor's Forwarding 533 screen, accounts can be set to forward messages to a specific smart host rather than using MDaemon's standard delivery process. By default, when MDaemon encounters a delivery error when attempting to forward one of those messages, it will be placed in the bad message queue. Enable this option if you instead want MDaemon to place the message into the Retry Queue 654 for further delivery attempts using MDaemon's normal delivery process.

Delete messages sent from blacklisted senders (otherwise put in bad queue)
Enable this option if you want MDaemon to delete incoming messages from senders who are in the recipient's personal Blacklist IMAP folder. When this option is disabled, the message will be placed into the Bad Message Queue instead of being deleted. This option is disabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

3.9.2 Windows Service



Windows Service

When MDaemon is running as a service, the service's name is "MDaemon."

Dependencies
Use this option to designate any services what you wish to require to be running **before** the MDaemon service starts.

Start service
This is the initial state of the service: automatically starts, must be started manually, or disabled.

Install/Remove service
Click this button to install or remove the MDaemon service.

Network Resource Access

When running MDaemon as a Windows service, by default it runs under the SYSTEM account. Because this account does not have access to network devices, MDaemon will not be able to access mail if you wish to store it on other computers across your LAN. That is, not unless you provide logon credentials for an account that can be used to provide the MDaemon service access to network shares. If you need to do this then you can create a Windows user account specifically designed for running MDaemon

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

with whatever restrictions that you desire, but which has access to those network shares that you want MDaemon to be able to use. Further, all applications launched by MDaemon will use the same credentials.

Logon name
This is the logon name of the Windows account under which the MDaemon service should run.

Password
This is the Windows account's password.

Domain
This is the Windows Domain on which the account resides. Leave this field blank to login to the default domain.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Section

4 Security Menu

MDaemon is equipped with an extensive suite of security features and controls. Click Security on MDaemon's menu bar to reach the following security features:

- **AntiVirus** 362 — SecurityPlus for MDaemon can help you stop email-borne computer viruses by providing the highest level of integrated protection available for MDaemon customers. It will catch, quarantine, repair, and/or remove any email message found to contain any virus. For MDaemon PRO users, SecurityPlus also contains a feature called Outbreak Protection, which can be used to protect you from certain spam, phishing, and virus outbreaks that can sometimes be missed by the other traditional, content and signature-based security measures.
- **Content Filter** 364 — a highly versatile and fully multi-threaded Content Filtering system makes it possible for you to customize server behavior based on the content of incoming and outgoing email messages. You can insert and delete message headers, add footers to messages, remove attachments, route copies to other users, cause an instant message to be sent to someone, run other programs, and much more.
- **Spam Filter** 401 — uses spam filtering technology to heuristically examine email messages in order to compute a "score". This score is used to determine the likelihood of a message being spam. Based on that determination the server can then take certain actions such as refusing or flagging the message. See also: Spam Traps 431
- **DNS Black Lists** 425 —allows you to specify several DNS blacklisting services that will be checked each time someone tries to send a message to your server. If the connecting IP has been blacklisted by any one of these hosts, the message will be refused.
- **Relay Control** 432 — used to control what MDaemon will do when a message arrives at your mail server that is neither from nor to a local address.
- **IP Shield** 440 — if a domain name specified in this list attempts to connect to your server, its IP address must match the one that you have assigned to it.
- **Reverse Lookup** 434 — MDaemon can query DNS servers to check the validity of the domain names and addresses reported during incoming messages. Controls on this screen can be used to cause suspicious messages to be refused or a special header inserted into them. Reverse Lookup data will also be reported in the MDaemon logs.
- **POP Before SMTP** 437 — the controls on this screen are used to require each user to first access his or her mailbox before being allowed to send a message through MDaemon, thus authenticating that the user is a valid account holder and allowed to use the mail system.
- **Trusted Hosts** 438 — domain names and IP addresses that will be considered as exceptions to the relay rules listed on the Relay Control screen.
- **SMTP Authentication** 442 — used for setting several options that denote how MDaemon will behave when a user sending a message to MDaemon has or has not been authenticated first.
- **SPF** 444 — Most domains publish MX records to identify the machines that may

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

receive mail for them, but this doesn't identify the locations allowed to send mail for them. Sender Policy Framework (SPF) is a means by which domains can also publish "reverse MX" records to identify those locations authorized to send messages.

- **DomainKeys Identified Mail** 446 — DomainKeys Identified Mail (DKIM) is an email verification system that can be utilized to prevent spoofing. It can also be used to ensure the integrity of incoming messages, ensuring that the message hasn't been tampered with between the time it left the sender's mail server and arrived at yours. This is accomplished by using an encrypted public/private key pairs system. Outgoing messages are signed using a private key and incoming messages have their signatures verified by testing them with the public key published on the sender's DNS server.
- **Certification** 469 — Message Certification is a process by which one entity vouches for or "certifies" the good email conduct of another entity. The Certification feature is beneficial because it can help ensure that messages will not be erroneously or needlessly subjected to unwarranted spam filter analysis. It can also help lower the resources required to process each message.
- **Sender Blacklist** 475 — lists addresses that are not allowed to send mail traffic through your server.
- **IP Screen** 478 — used to designate IP addresses from which you will allow or refuse connections to your server.
- **Host Screen** 480 — used to designate hosts (domain names) from which you will allow or refuse connections to your server.
- **Dynamic Screen** 482 — using the Dynamic Screening feature, MDaemon can track the behavior of sending servers to identify suspicious activity and then respond accordingly. For example, you can temporarily ban an IP address from future connections to your server once a specified number of "unknown recipient" errors occur during the mail connection from that IP address.
- **SSL & TLS** 487 — MDaemon supports the Secure Sockets Layer (SSL) protocol for SMTP, POP, and IMAP, and for WorldClient's web server. SSL is the standard method for securing server/client Internet communications.
- **Backscatter Protection** 502 — "Backscatter" refers to response messages that your users receive to emails that they never sent. This occurs when spam messages or messages sent by viruses contain a Return-Path address that is forged. Backscatter Protection helps prevent this by ensuring that only legitimate Delivery Status Notifications and Autoresponders get delivered to your accounts, by using a private key hashing method to generate and insert a special time-sensitive code into the Return-Path address of your users' outgoing messages.
- **Bandwidth Throttling** 506 — the Bandwidth Throttling feature makes it possible for you to police the consumption of bandwidth used by MDaemon. You can control the rate at which sessions or services progress, setting different rates for each of MDaemon's major services on a per-domain basis, including Domains and Domain Gateways.
- **Tarpitting** 508 — makes it possible for you to deliberately slow down a connection once a specified number of RCPT commands have been received from a message's sender. This is to discourage spammers from trying to send

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

unsolicited bulk email to you. The assumption behind this technique is that if takes spammers an inordinately long period of time to send each message then that will discourage them from trying to do so again in the future.

- **Greylisting** 510 — Greylisting is a spam-fighting technique that exploits the fact that SMTP servers retry delivery of any message that receives a temporary (i.e. "try again later") error code. Using this technique, when a message arrives from a non-white listed or otherwise previously unknown sender, its sender, recipient, and sending server's IP address will be logged and then the message will be refused by Greylisting with a temporary error code during the SMTP session. Then, when the legitimate servers attempt to deliver the messages again a few minutes later, they will be accepted. Because spammers do not typically make further delivery attempts, Greylisting can significantly help to reduce the amount of spam your users receive.
- **LAN IPs** 514 — use this screen to list IP addresses that reside on your LAN (local area network). These IP addresses are therefore treated as local traffic for the purposes of bandwidth throttling, and may be exempt from various other security and spam prevention restrictions.
- **Site Policy** 515 — used for creating a site policy to be transmitted to sending servers at the beginning of every SMTP mail session. An example of a common site policy is, "This server does not relay."

4.1 Content Filter and AntiVirus

Content Filter

The Content Filter 364 (Security » Content Filter) can be used for a large number of purposes such as: preventing spam email, intercepting messages containing viruses before they reach their final destination, copying certain emails to one or more additional users, appending a note or disclaimer to the bottom of messages, adding, and deleting headers, stripping email attachments, deleting messages, and more. Because individual Content Filter rules are created by the administrator, and because of their diversity, they can be used in many situations and are limited for the most part only be the creativity of the person creating them. With a little bit of thought and experimentation, this feature can be very useful.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

SecurityPlus for MDaemon

SecurityPlus
This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program or any portion of it, may result in severe criminal and civil penalties, and will be prosecuted to the maximum extent possible under law.
Copyright © 1996-2014 Alt-N Technologies, Ltd.
Alt-N Technologies®, MDaemon®, WorldClient®, and related trademarks are the property of Alt-N Technologies, Ltd. and are registered and/or used in the U.S. and countries around the world.
alt-n technologies

In a joint effort with Kaspersky Labs, a world-renowned anti-virus software developer, Alt-N Technologies has developed SecurityPlus for MDaemon, an anti-virus engine that can be installed and integrated with MDaemon. When SecurityPlus is installed you will see two additional tabs on the Content Filter dialog: AntiVirus 383 and AV Updater 386. These tabs are used to directly control the product's features and designate what actions MDaemon will take when a virus is detected. For MDaemon PRO users, SecurityPlus also contains a feature called Outbreak Protection 389, which is not heuristics-based or signature dependent like the traditional protection tools, but is designed to catch spam, phishing and virus attacks that are part of an ongoing outbreak, and which can sometimes by missed by the traditional tools. To obtain SecurityPlus for MDaemon, visit www.altn.com.

See:

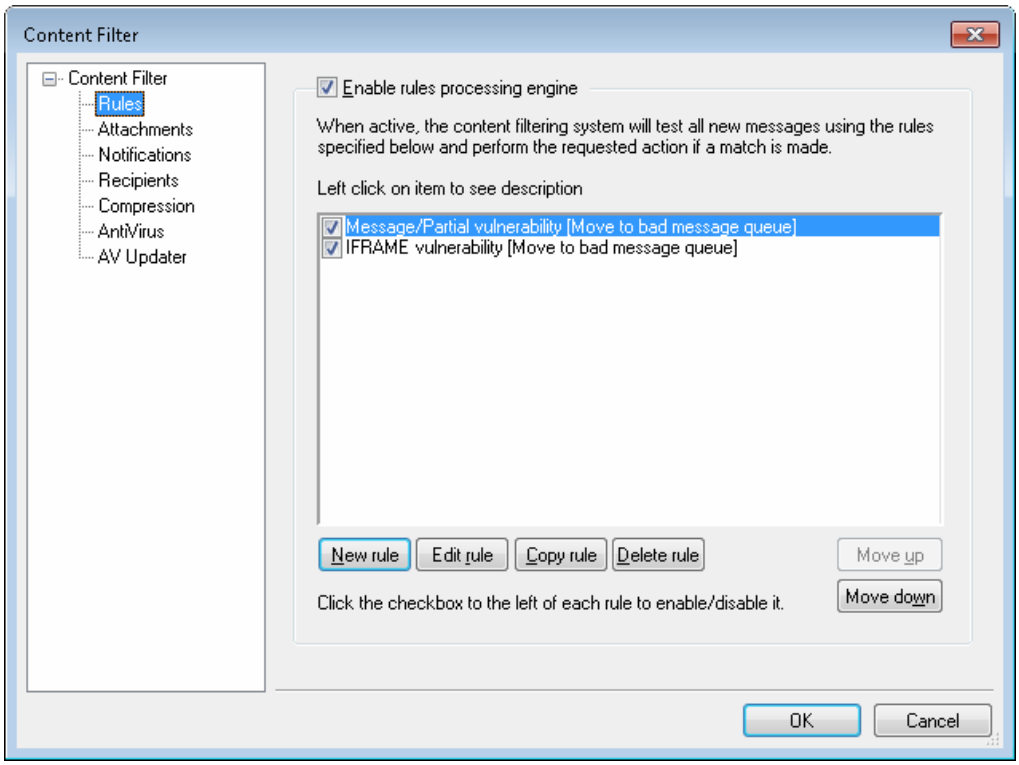
Content Filter Editor 364
Creating a New Content Filter Rule 366
Modifying an Existing Content Filter Rule 370
Using Regular Expressions in Your Filter Rules 370

AntiVirus 383
AntiVirus Updater 386
Outbreak Protection 389

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.1.1 Content Filter Editor

4.1.1.1 Rules



All messages processed by MDaemon will at some point reside temporarily in one of the message queues. When Content Filtering is enabled, before any message is allowed to leave the queue it will first be processed through the Content Filter rules. The result of this procedure will determine what is done with the message.

Messages that have a filename beginning with the letter "P" will be ignored by the content filtering process. Every other message will be processed through the content filter system. Once processed, MDaemon will change the first character of the filename to a "P". In this way a message will only be processed through the content filtering system once.

Content Filtering Rules

Enable rules processing engine
Click this checkbox to enable content filtering. All messages processed by MDaemon will be filtered through the content filter rules before being delivered.

Existing Content Filtering Rules

This box lists all of your Content Filter rules, with a checkbox beside each one so that you can enable/disable them at will. To see a description of any given rule in its internal script format, click that rule and pause your mouse-cursor over it (moving

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

your mouse will cause the description to disappear). Whenever a message is processed through the Content Filter, these rules will be applied in the order in which they are listed. This makes it possible for you to arrange your rules to achieve a greater level of versatility.

For example: If you have a rule that deletes all messages containing the words, "This is Spam!" and a similar rule that sends those messages to the Postmaster, then putting them in the right order will enable both rules to be applied to the message. This assumes that there isn't a "Stop Processing Rules" rule that applies to the message higher up in the list. If so, then you would use the *Move Up*/*Move Down* buttons to move the "Stop" rule below the other two. Then, any message containing "This is Spam!" would be copied to the Postmaster and then deleted.

MDaemon has the capability to create rules that will perform multiple tasks and use `and/or` logic. Considering the example above, instead of using multiple rules you could create a single rule that would accomplish all of those tasks and more.

New rule
Click this button to create a new content filter rule. This will open the Create Rule 366 dialog.

Edit rule
Click this button to open the selected rule in the Modify Rule 370 editor.

Copy rule
Click this button to clone the selected content filter rule. An identical rule will be created and added to the list. The new rule will be given a default name of "Copy of [Original Rule Name]". This is useful if you wish to create multiple similar rules. You can create a single rule, clone it several times, and then modify the copies as needed.

Delete rule
Click this button to delete the selected content filter rule. You will be asked to confirm your decision to delete the Rule before MDaemon will do so.

Move up
Click this button to move the selected rule up.

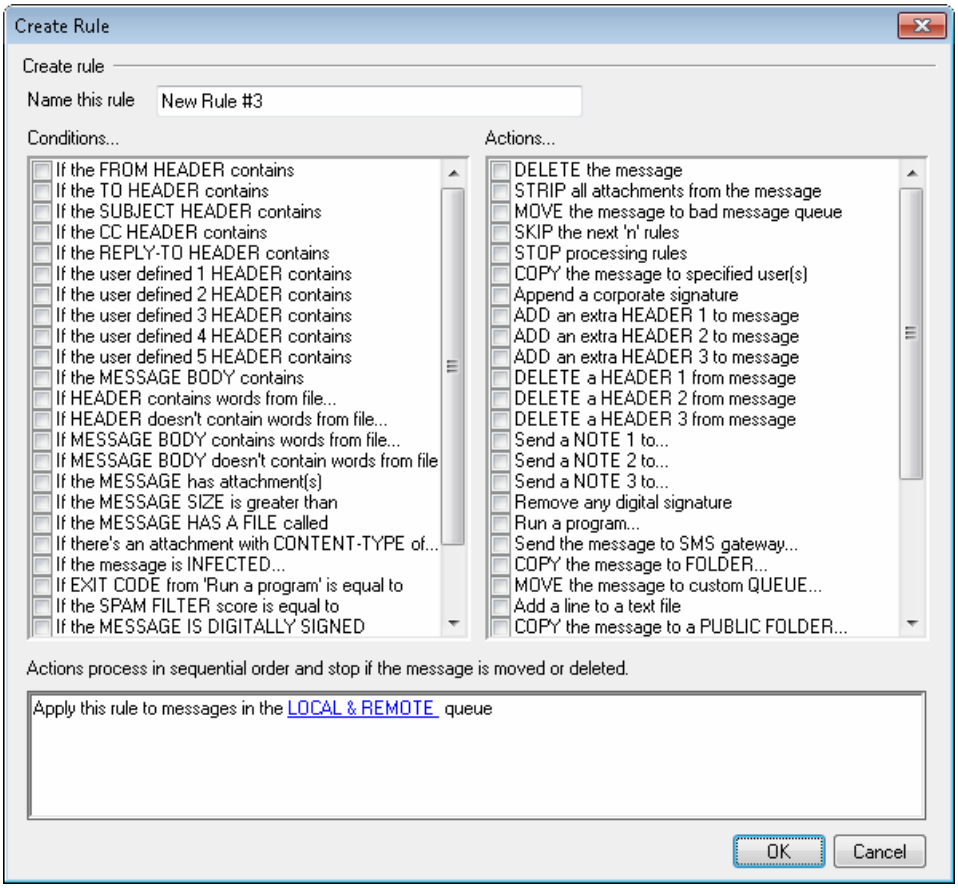
Move down
Click this button to move the selected rule down.

See:

Creating a New Content Filter Rule 366
Modifying an Existing Content Filter Rule 370
Using Regular Expressions in Your Filter Rules 370

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.1.1.1.1 Creating a New Content Filter Rule


Create Rule
Create rule
Name this rule
New Rule #3
Conditions...
If the FROM HEADER contains
If the TO HEADER contains
If the SUBJECT HEADER contains
If the CC HEADER contains
If the REPLY-TO HEADER contains
If the user defined 1 HEADER contains
If the user defined 2 HEADER contains
If the user defined 3 HEADER contains
If the user defined 4 HEADER contains
If the user defined 5 HEADER contains
If the MESSAGE BODY contains
If HEADER contains words from file...
If HEADER doesn't contain words from file...
If MESSAGE BODY contains words from file...
If MESSAGE BODY doesn't contain words from file
If the MESSAGE has attachment(s)
If the MESSAGE SIZE is greater than
If the MESSAGE HAS A FILE called
If there's an attachment with CONTENT-TYPE of...
If the message is INFECTED...
If EXIT CODE from 'Run a program' is equal to
If the SPAM FILTER score is equal to
If the MESSAGE IS DIGITALLY SIGNED
Actions...
DELETE the message
STRIP all attachments from the message
MOVE the message to bad message queue
SKIP the next 'n' rules
STOP processing rules
COPY the message to specified user(s)
Append a corporate signature
ADD an extra HEADER 1 to message
ADD an extra HEADER 2 to message
ADD an extra HEADER 3 to message
DELETE a HEADER 1 from message
DELETE a HEADER 2 from message
DELETE a HEADER 3 from message
Send a NOTE 1 to...
Send a NOTE 2 to...
Send a NOTE 3 to...
Remove any digital signature
Run a program...
Send the message to SMS gateway...
COPY the message to FOLDER...
MOVE the message to custom QUEUE...
Add a line to a text file
COPY the message to a PUBLIC FOLDER...
Actions process in sequential order and stop if the message is moved or deleted.
Apply this rule to messages in the LOCAL & REMOTE queue
OK
Cancel

This dialog is used for creating Content Filter Rules. It is reached by clicking the *New Rule* button on the Content Filter dialog.

Create Rule

Name this rule
Type a descriptive name for your new rule here. By default it will be called "New Rule #n".

Conditions...

This box lists the conditions that may be applied to your new rule. Click the checkbox corresponding to any condition that you want to be applied to the new rule. Each enabled condition will appear in the Rule Description box below. Most Conditions will require additional information that you will specify by clicking on the Condition's hyperlink in the Rule Description box.

`If the [HEADER] contains`—Click any of these options to base your rule on the content of those particular message headers. You must specify the text for which to scan. This condition now supports regular expressions. See Using Regular Expressions in Your Filter Rules 370.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

If the user defined [# HEADER] contains—Click one or more of these options to base the rule on message headers that you will define. You must specify the new header, and the text for which to scan. This condition now supports regular expressions. See Using Regular Expressions in Your Filter Rules 370.

If the MESSAGE BODY contains—This option makes the contents of the message body one of the conditions. This condition requires you to specify a text string for which to search. This condition now supports regular expressions. See Using Regular Expressions in Your Filter Rules 370.

If the MESSAGE has Attachment(s)—When this option is selected, the rule will be contingent upon the presence of one or more message attachments. No additional information is required.

If the MESSAGE SIZE is greater than—Click this option if you want the rule to be based upon the size of the message. The size must be specified in *KB*. Default is 10KB.

If the MESSAGE HAS A FILE called—This option will scan for a file attachment with a particular name. The filename must be specified. Wildcards such as *.exe and file *.* are permitted.

If message is INFECTED...—This condition is `TRUE` when SecurityPlus for MDaemon determines that a message is infected with a virus.

If the EXIT CODE from a previous run process is equal to—If a previous rule in your list utilizes the *Run Process* action, you can use this condition to look for a specific exit code from that process.

If the MESSAGE IS DIGITALLY SIGNED—The condition applies to messages that have been digitally signed. No further information is required by this condition.

If SENDER is a member of GROUP...—This condition applies to a message when it is sent by an account that is a member of the account Group designated in the rule.

If RECIPIENT is a member of GROUP...— This condition applies to a message when its recipient is a member of the account Group designated in the rule.

If ALL MESSAGES—Click this option if you want the rule to be applied to all messages. No further information is required; this rule will affect every message except those to which a "Stop Processing Rules" or "Delete Message" action has been applied in a previous rule.

Actions...

MDaemon can perform these actions if a message matches the rule's conditions. A few Actions will require additional information that you will specify by clicking on the Action's hyperlink in the Rule Description box.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Delete Message—Selecting this action will cause the message to be deleted.

Strip All Attachments From Message—This action causes all attachments to be stripped from the message.

Move Message To Bad Message Queue—Click this action to cause a message to be moved to the bad message queue. An `X-MDBadQueue-Reason` header will be added to the message.

Skip n Rules—Selecting this action will cause a specified number of rules to be skipped. This is useful in situations where you may want a rule to be applied in certain circumstances but not in others.

For example: you may wish to delete messages that contain the word "Spam", but not those that contain "Good Spam". To accomplish this you could create a rule that deletes messages containing "Spam" and then place above it another rule that states "if the message contains "Good Spam" then Skip 1 Rule".

Stop Processing Rules—This action will skip all remaining rules.

Copy Message To Specified User(s)—Causes a copy of the message to be sent to one or more recipients. You must specify which recipients are to receive the message.

Append a corporate signature—This action makes it possible for you to create a small amount of text that will be appended as a footer to the message. Alternatively, it can add the contents of a text file. There is a *Use HTML* checkbox available if you wish to include HTML code in your signature's text.

For example: you could use this rule to include a statement that says "This email originated from my company, please direct any complaints or questions to user01@example.com".

Add Extra Header Item To Message—This action will add an additional header to the message. You must specify the name of the new header and its value.

Delete A Header Item From Message—This action will remove a header from a message. You must specify the header that you wish to delete.

Send Note To... —This action will send an email to a particular address. You will be able to specify the recipient, sender, subject, and a small amount of text. You can also configure this action to attach the original message to the note.

For example: you might wish to create a rule that will move all messages containing "This is Spam!" to the bad message directory and create another rule that will send a note to someone letting them know that this has been done.

Remove Digital Signature—Click this action to cause a digital signature to be removed from the message.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Run Process...—This action can be used to run a particular program when a message meets the rule's conditions. You must specify the path to the program that you wish to run. You can use the $MESSAGEFILENAME$ macro to pass the name of the message to the process, and you can specify whether or not MDaemon should suspend its operations temporarily or indefinitely while it waits for the process to terminate. Further, you can force the process to terminate and/or run it in a hidden window.

Send Message Through SMS Gateway Server...—Click this option to send the message through an SMS Gateway Server. You must supply the Host or IP Address and the SMS phone number.

Copy Message to Folder...—Use this option to place a copy of the message into a specific folder.

MOVE the messages to custom QUEUE...—Use this action to move the message into one or more previously created custom mail queues. When moving messages to custom remote mail queues you can use the custom scheduling options on the Event Scheduler to control when those messages will be processed.

Add Line To Text File—This option will cause a line of text to be added to a specific text file. When choosing this action you will have to specify the path to the file and the text that you want to be appended to it. You may use certain MDaemon macros in your text to cause the content filter to dynamically include information about the message such as the sender, recipient, message ID, and so on. Click the Macros button on the "Add line to text file" dialog to display a list of permitted macros.

Move Message to Public Folders...—Use this action to cause the message to be moved to one or more Public Folders.

Search and Replace Words in a Header—Use this option to scan a specified header for certain words and then delete or replace them. When creating this rule, click the "specify information" link in the Rule Description to open the "Header – Search and Replace" dialog on which you will designate the header and words to replace or delete. This action now supports regular expressions. See Using Regular Expressions in Your Filter Rules 370.

Search and Replace Words in the Message Body—Use this option to scan the message body and replace any desired text. This action now supports regular expressions. See Using Regular Expressions in Your Filter Rules 370.

Jump to Rule...—Use this action to jump immediately to a rule further down in the list, skipping over all rules between the two.

Sign with DKIM selector...—Use this action if you want the rule to cause a message to contain a DKIM signature 450. You can also use it if you wish to sign some messages using a selector other than the one designated on the DKIM dialog.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Rule description
This box displays the new rule's internal script format. Click any of the rule's conditions or actions (listed as hyperlinks) and the appropriate editor will be opened for specifying any needed information.

See:

Content Filter Editor 364
Modifying an Existing Content Filter Rule 370
Using Regular Expressions in Your Filter Rules 370

4.1.1.1.2 Modifying an Existing Content Filter Rule

To modify an existing content filter rule, select the rule and then click the *Edit Rule* button on the Content Filter dialog. The rule will be opened for editing in the Modify Rule editor. The controls on this editor are identical to the Create Rule Dialog 366.

See:

Content Filter Editor 364
Creating a New Content Filter Rule 366
Using Regular Expressions in Your Filter Rules 370

4.1.1.1.3 Using Regular Expressions in Your Filter Rules

The Content Filtering system supports *regular expression* searches, which is a versatile system that makes it possible for you to search not only for specific text strings, but also for text *patterns*. Regular expressions contain a mix of plain text and special characters that indicate what kind of matching to do, and can thus make your Content Filter rules more powerful and better targeted.

What are Regular Expressions?
A regular expression (regexp) is a text pattern consisting of a combination of special characters known as *metacharacters* and alphanumeric text characters, or "*literals*" (abc, 123, and so on). The pattern is used to match against text strings—with the result of the match being either successful or not. Regexps are used primarily for regular text matches and for search and replace.

Metacharacters are special characters that have specific functions and uses within regular expressions. The regexp implementation within the MDaemon Content Filtering system allows the following metacharacters:

```
\ | () [] ^ $ * + ? . <>
```

Metacharacter	Description
\	When used before a metacharacter, the backslash ("\")

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

causes the metacharacter to be treated as a literal character. This is necessary if you want the regular expression to search for one of the special characters that are used as metacharacters. For example, to search for "+" your expressions must include "\+".

| The *alternation* character (also called "*or*" or "*bar*") is used when you want either expression on the side of the character to match the target string. The regexp "abc|xyz" will match any occurrence of either "abc" or "xyz" when searching a text string.

[...] A set of characters contained in brackets ("[" and "]") means that any character in the set may match the searched text string. A dash ("-") between characters in the brackets denotes a range of characters. For example, searching the string "abc" with the regexp "[a-z]" will yield three matches: "*a*," "*b*, " and "*c*. " Using the expression "[az]" will yield only one match: "*a*."

^ Denotes the beginning of the line. In the target string, "abc ab a" the expression "^a" will yield one match—the first character in the target string. The regexp "^ab" will also yield one match—the first *two* characters in the target string.

[^...] The caret ("^") immediately following the left-bracket ("[") has a different meaning. It is used to exclude the remaining characters within brackets from matching the target string. The expression "[^0-9]" indicates that the target character should not be a digit.

(...) The parenthesis affects the order of pattern evaluation, and also serves as a *tagged* expression that can be used in *search and replace* expressions.

The results of a search with a regular expression are kept temporarily and can be used in the *replace* expression to build a new expression. In the *replace* expression, you can include a "&" or "\0" character, which will be replaced by the sub-string found by the regular expression during the search. So, if the *search* expression "a(bcd)e" finds a sub-string match, then a *replace* expression of "123-&-123" or "123-\0-123" will replace the matched text with "123-abcde-123".

Similarly, you can also use the special characters "\1," "\2," "\3," and so on in the *replace* expression. These characters will be replaced only be the results of the *tagged* expression instead of the entire sub-string match. The number following the backslash denotes which tagged expression you wish to reference (in the case of a regexp containing

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

more than one tagged expression). For example, if your *search* expression is "(123)(456)" and your *replace* expression is "a-\2-b-\1" then a matching sub-string will be replaced with "a-456-b-123" whereas a *replace* expression of "a-\0-b" will be replaced with "a-123456-b"

**$** The dollar sign ("$") denotes the end of the line. In the text string, "13 321 123" the expression "3$" will yield one match —the last character in the string. The regexp "123$" will also yield one match—the last *three* characters in the target string.

***** The asterisk ("*") quantifier indicates that the character to its left must match *zero or more* occurrences of the character in a row. Thus, "1*abc" will match the text "111abc" and "abc."

+ Similar to the asterisk quantifier, the "+" quantifier indicates that the character to its left must match *one or more* occurrences of the character in a row. Thus, "1+abc" will match the text "111abc" but not "abc."

? The question mark ("?") quantifier indicates that the character to its left must match *zero or one* times. Thus, "1?abc" will match the text "abc," and it will match the "1abc" portion of "111abc."

. The period or dot (".") metacharacter will match any other character. Thus ".+abc" will match "123456abc," and "a.c" will match "aac," abc," acc," and so on.

Eligible Conditions and Actions
Regular expressions may be used in any *Header* filter rule *Condition*. For example, any rule using the "`if the FROM HEADER contains`" condition. Regular expressions may also be used in the "`if the MESSAGE BODY contains`" condition.

Regular expressions may be used in two Content Filter rule *Actions*: "`Search and Replace Words in a Header`" and "`Search and Replace Words in the Message Body`."

Regular expressions used in Content Filter rule *conditions* are case insensitive. Case will not be considered.

Case sensitivity in regular expressions used in Content Filter rule *actions* is optional. When creating the regexp within the rule's action you will have the option to enable/disable case sensitivity.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Configuring a Regexp in a Rule's Condition

To configure a header or message body condition to use a regular expression:

1. On the Create Rule dialog, click the checkbox that corresponds to the header or message body condition that you wish to insert into your rule.

2. In the summary area at the bottom of the Create Rule dialog, click the "**contains specific strings**" link that corresponds to the condition that you selected in step 1. This will open the Specify Search Text dialog.

3. Click the "**contains**" link in the "Currently specified strings..." area.

4. Choose "**Matches Regular Expression**" from the drop-down list box, and click **OK**.

5. If you need help creating your regexp or want to test it then click "**Test regular expression**." If you do not need to use the Test Regular Expression dialog then type your regexp into the text box provided, click **Add**, and then go to step 8.

6. Type your regular expression into the "Search expression" text box. To simplify the process we have provided a shortcut menu that can be used to easily insert the desired metacharacters into your regexp. Click the ">" button to access this menu. When you choose an option from this menu its corresponding metacharacter will be inserted into the expression and the text insertion point will be moved to the appropriate place required by the character.

7. Type any text that you wish to use to test your expression in the text area provided, and click **Test**. When you are finished testing your expression, click **OK**.

8. Click **OK**.

9. Continue creating your rule normally.

Configuring a Regexp in a Rule's Action

To configure a "Search and Replace Words in…" action to use a regular expression:

1. On the Create Rule dialog, click the checkbox that corresponds to the "*Search and Replace Words in...*" action that you wish to insert into your rule.

2. In the summary area at the bottom of the Create Rule dialog, click the "**specify information**" link that corresponds to the action that you selected in step 1. This will open the Search and Replace dialog.

3. If you chose the "*Search...header*" action in step 1, then use the drop-down list box provided to choose the header that you wish to search, or type a header into the box if the desired header isn't listed. If you did not choose the "*Search...header*" action in step 1 then skip this step.

4. Type the *search* expression that you wish to use in this action. To simplify the process we have provided a shortcut menu that can be used to easily insert the desired metacharacters into your regexp. Click the ">" button to access this menu.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

When you choose an option from this menu its corresponding metacharacter will be inserted into the expression and the text insertion point will be moved to the appropriate place required by the character.

5. Type the *replace* expression that you wish to use in this action. As with the *search* expression we have provided a metacharacter shortcut menu for this option as well. Leave this text box blank if you wish to delete a matched sub-string instead of replace it with more text.

6. Click "**Match case**" if you want the expression to be case sensitive.

7. Click Regular expression if you want the search and replace strings to be treated as regular expressions. Otherwise each will be treated as a simple sub-string search and replace—it will look for an exact literal match of the text rather than process it as a regular expression.

8. If you do not need to test your expression then skip this step. If you do need to test your expression then click "**Run Test**." On the Search and Replace Tester dialog, type your search and replace expressions and the text that you wish to test with, then click **Test**. When you are finished testing your regexps click **OK**.

9. Click **OK**.

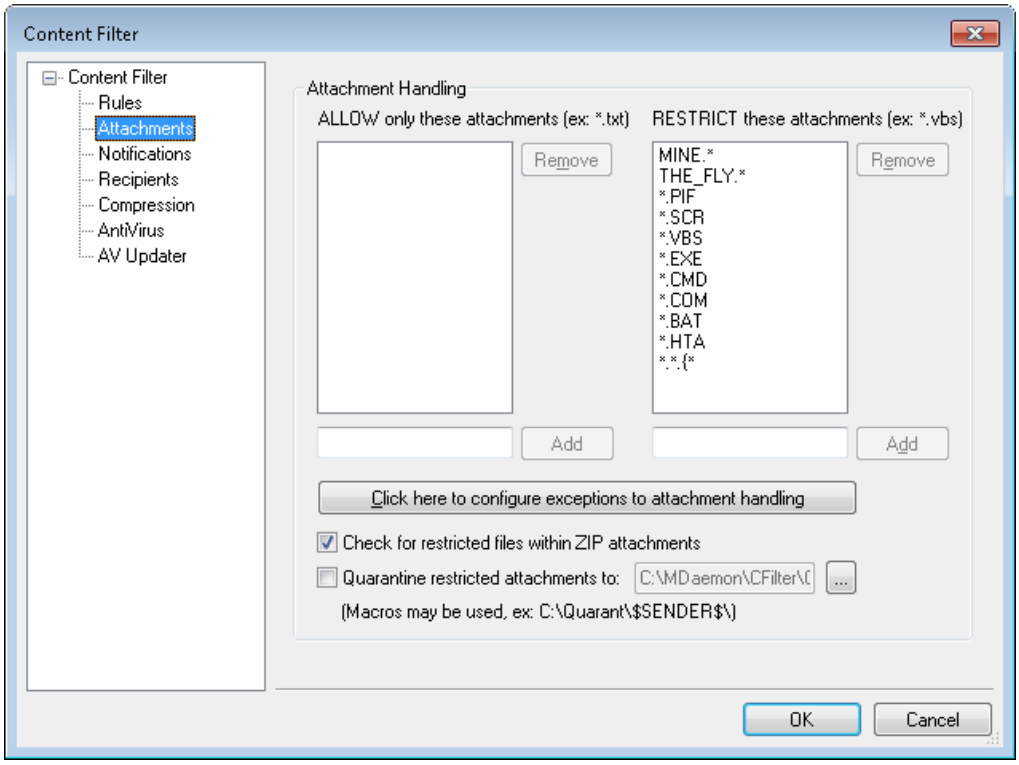
10. Continue creating your rule normally.

MDaemon's regexps implementation uses the PERL Compatible Regular Expression (PCRE) library. You can find more information on this implementation of regexps at: http://www.pcre.org/ and http://perldoc.perl.org/perlre.html.

For a comprehensive look at regular expressions, see: *Mastering Regular Expressions, Third Edition* published by O'Reilly Media, Inc.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.1.1.2 Attachments



Use this tab to specify attachments that you wish to classify as allowed or restricted. Attachments that are not allowed will be automatically removed from messages.

Attachment Handling

Filenames specified in *RESTRICT these attachments* list will be stripped from messages automatically when MDaemon encounters them. If you list any files in the *ALLOW only these attachments* list, then only those files listed will be permitted — all other attachments will be stripped from messages. After the attachment is stripped, MDaemon will continue normally and delivery the message without it. You can use the options on the Notifications tab to cause a notification message to be sent to various addresses when one of these restricted attachments is encountered.

Wildcards are permitted in list entries. An entry of "`*.exe`", for example, would cause all attachments ending with the `EXE` file extension to be allowed or removed. To add an entry to either of the lists, type the filename in the space provided and the click Add.

Click here to configure exceptions to attachment handling
Click this button to specify addresses that you wish to exclude from attachment restriction monitoring. When a message is directed to one of these addresses MDaemon will allow the message to pass even if it contains a restricted attachment.

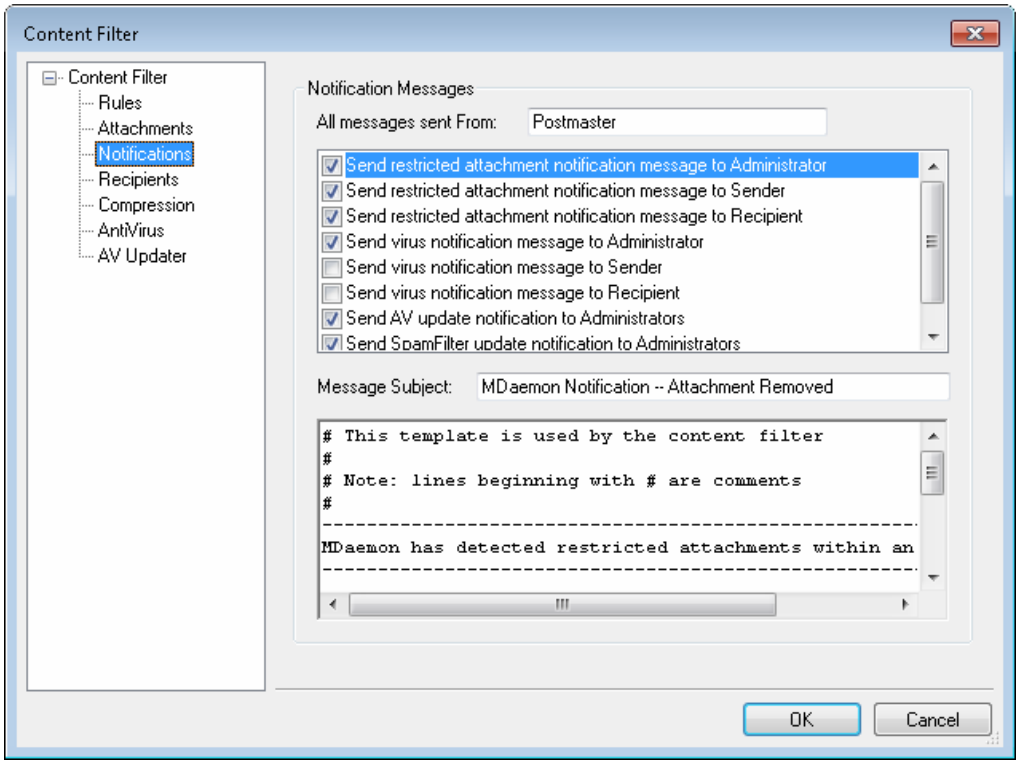
Check for restricted files within ZIP attachments
Click this option if you wish to scan the contents of zipped files for restricted attachments. Additionally, any Content Filter rule set to look for a particular filename

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

will be triggered if a matching file is found within a zipped attachment.

Quarantine restricted attachments to:
Click this option and specify a location if you wish to quarantine restricted attachments to a specific location rather than simply delete them.

4.1.1.3 Notifications



Use this screen to designate those who should receive notification messages when a virus or restricted attachment is detected, or when the antivirus or Spam Filter files are updated.

Notification Messages

All messages sent From:
Use this box for specifying the address from which you wish the notification messages to be sent.

Send virus notification message to...
When a message arrives with a file attachment containing a virus, a warning message will be sent to the individuals designated in this section. A customized warning message can be sent to the sender, recipient, and the administrators that you have designated on the Recipients 380 screen. To customize the message for any of the three entries, select one of them from the list and then edit the message that appears on the bottom half of this screen. Each entry has its own message, though by default this isn't obvious since some are identical.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Send restricted attachment notification message to...
When a message arrives with a file attachment matching a restricted attachment entry (listed on the Attachments tab) a warning message will be sent to the individuals designated in this section. A customized warning message can be sent to the sender, recipient, and the administrators that you have designated on the Recipients tab. To customize the message for any of the three entries, select one of them from the list and then edit the message that appears on the bottom half of this tab. Each entry has its own message, though by default this isn't obvious since all three are identical.

Send Spam Filter update notification to Administrators
Use this option if you wish to send an email to the administrators whenever the Spam Filter is updated, containing the results of the update. This option is the same as the "*Send notification email with results of update*" option located at: `Spam Filter » Updates`.

Message Subject:
This text will be displayed in the "Subject:" header of the notification message that is sent.

Message
This is the message that will be sent to the entry selected in the list above when the checkbox corresponding to that entry is enabled. You can directly edit this message from the box in which it is displayed.

The actual files containing this text are located in the `MDaemon \app\` directory. They are:

`cfattrem[adm].dat` – Restricted attachment message – Admins
`cfattrem[rec].dat` – Restricted attachment message – Recipient
`cfattrem[snd].dat` – Restricted attachment message – Sender
`cfvirfnd[adm].dat` – Virus found message – Admins
`cfvirfnd[rec].dat` – Virus found message – Recipient
`cfvirfnd[snd].dat` – Virus found message – Sender

Should you desire to restore one of these messages to its original appearance, simply delete the relevant file and MDaemon will recreate it in its default state.

4.1.1.3.1 Message Macros

For your convenience, certain macros may be used in the notification messages and other messages that the Content Filters generate. You may use any of the following macros:

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

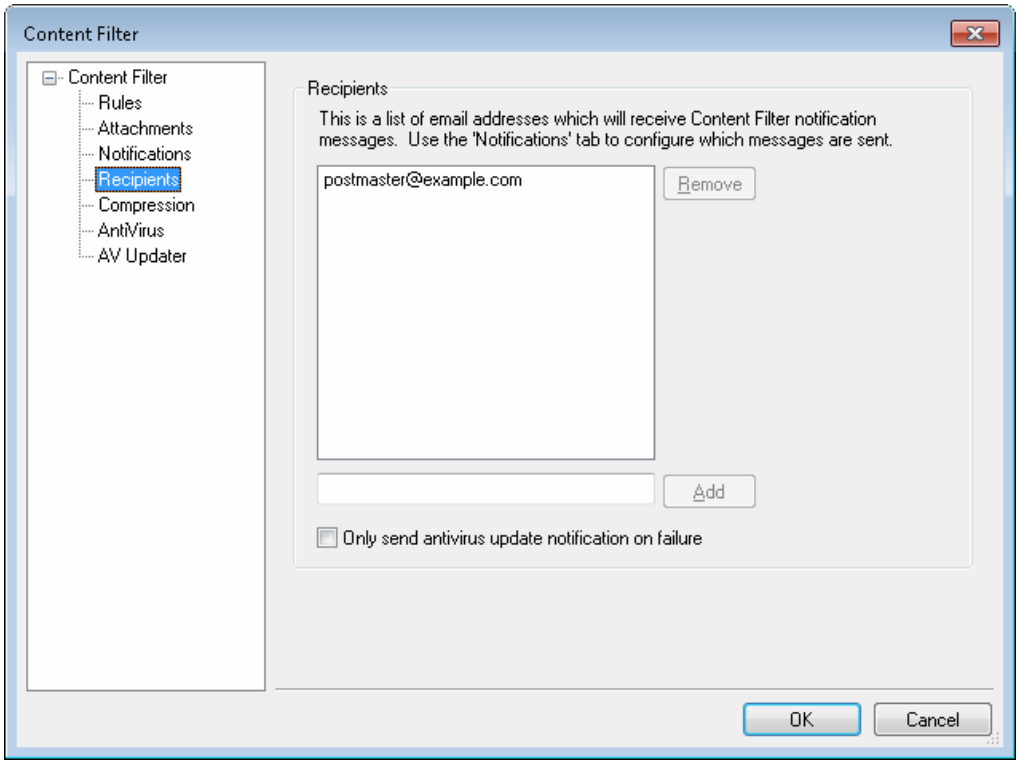
$ACTUALTO$	Some messages may contain an "ActualTo" field which generally represents the destination mailbox and host as it was entered by the original user prior to any reformatting or alias translation. This macro is replaced with that value.
$AV_VERSION$	Lists the version of SecurityPlus for MDaemonthat you are using.
$CURRENTTIME$	This macro is replaced with the current time when the message is being processed.
$ACTUALFROM$	Some messages may contain an "ActualFrom" field which generally represents the origination mailbox and host prior to any reformatting or alias translation. This macro is replaced with that value.
$FILTERRULENAME$	This macro is replaced by the name of the rule whose criteria the message matched.
GEN_GUID	Generates a unique ID with 11 alpha-numeric characters. Example: 0XVBASADTZC
$HEADER:XX$	This macro will cause the value of the header specified in place of the "xx" to be expanded in the reformatted message. For example: If the original message has "TO: user01@example.com" then the $HEADER:TO$ macro will expand to "user01@example.com". If the original message has "Subject: This is the subject" then the $HEADER:SUBJECT$ macro would be replaced with the text "This is the subject"
$HEADER:MESSAGE-ID$	As with $HEADER:XX$ above, this macro will expand to the value of the Message-ID header.
$LIST_ATTACHMENTS_REMOVED$	When one or more attachments are removed from the message, this macro will list them.
$LIST_VIRUSES_FOUND$	When one or more viruses is found in a message, this macro will list them.
$MESSAGEFILENAME$	This macro expands to the file name of the current message being processed.
$MESSAGEID$	As $HEADER:MESSAGE-ID$ above, except this macro strips "<>" from the value of the message ID.
$PRIMARYDOMAIN$	Expands to MDaemon's Default Domain name, which is designated on the Domain Manager 121.
$PRIMARYIP$	This macro expands to the IPv4 address 124 of

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

	your Default Domain 121.
$PRIMARYIP6$	This macro expands to the IPv6 address 124 of your Default Domain 121.
$RECIPIENT$	This macro resolves to the full address of the message recipient.
$RECIPIENTDOMAIN$	This macro will insert the domain name of the message recipient.
$RECIPIENTMAILBOX$	Lists the recipient's mailbox (the value to the left of "@" in the email address).
$REPLYTO$	This macro expands to the value of the message's "Reply-to" header.
$SENDER$	Expands to the full address from which the message was sent.
$SENDERDOMAIN$	This macro will insert the domain name of the message's sender (the value to the right of "@" in the email address).
$SENDERMAILBOX$	Lists the sender's mailbox (the value to the left of "@" in the email address).
$SUBJECT$	Displays the text contained in the message's subject.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.1.1.4 Recipients



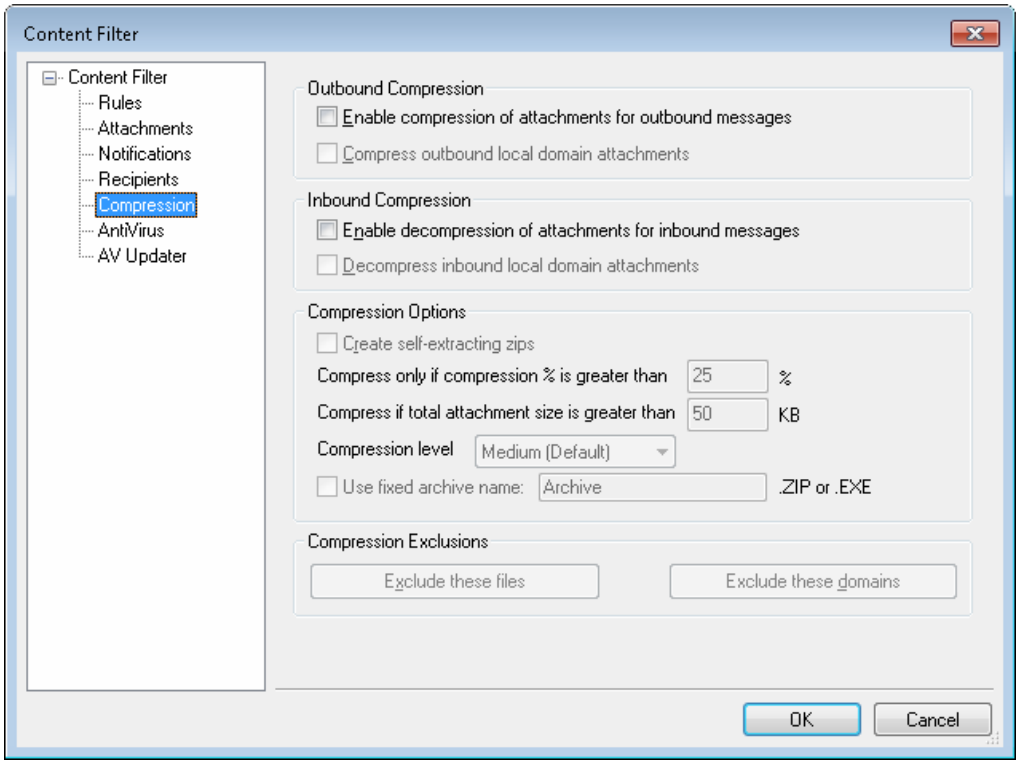
Recipients

This list of recipients corresponds to the various "*send...to administrator*" options located on the Notifications tab. These addresses will receive notification messages when one of the Administrator options is selected on that tab. To add an address to this section, type it into the space provided and then click *Add*. To remove an address, select it from the list and then click *Remove*.

Only send antivirus update notification on failure
Click this checkbox if you wish to send antivirus update notification messages only when the update attempt fails for some reason.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.1.1.5 Compression



With the controls on this tab you can cause message attachments to be automatically compressed or decompressed before the message is delivered. The level of compression can be controlled as well as several other parameters and exclusions. This feature could significantly reduce the amount of bandwidth and throughput required to deliver your outbound messages.

Outbound Compression

Enable compression of attachments for outbound messages
Click this checkbox if you want to enable automatic message attachment compression for outbound remote mail messages. Enabling this control will not cause all message attachments to be compressed; it simply turns the feature on. Whether an outbound message's files are compressed or not is determined by the remaining settings on this tab.

Compress outbound local domain attachments
Enabling this control will cause the file compression settings to be applied to all outbound mail – even those messages whose destination is another local address.

Inbound Compression

Enable decompression of attachments for inbound messages
Click this checkbox if you want to enable automatic decompression of inbound remote mail message attachments. When a message arrives with a zipped attachment, MDaemon will decompress it before delivering it to the local user's mailbox.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Decompress inbound local domain attachments
Enable this control if you want automatic decompression to apply to local mail as well.

Compression Options

Create self-extracting zips
Click this checkbox if you want the compression files that MDaemon creates to be self-extracting zip files with an `EXE` file extension. This is useful if you are concerned that the message recipients may not have access to a decompression utility. Self-extracting zip files can be decompressed simply by double-clicking on them.

Compress only if compression % is greater than XX%
MDaemon will not compress a message's attachments before sending it unless they can be compressed by a percentage greater than the value specified in this control. For example, if you designate a value of 20 and a given attachment can't be compressed by at least 21% then MDaemon will not compress it before sending the message.

MDaemon must first compress a file to determine by what percentage it can be compressed. Thus, this feature does not prevent files from being compressed – it simply prevents file attachments from being sent in a compressed format when they cannot be compressed beyond the designated value. In other words, if after compressing the file MDaemon finds that it couldn't be compressed by more than this value, the compression will be disregarded and the message will be delivered with its attachments unchanged.

Compress if total attachment size is greater than XX KB
When automatic attachment compression is enabled, MDaemon will only attempt to compress a message's attachments when their total size exceeds the value specified here. Messages with total attachment sizes below this threshold will be delivered normally with the attachments unchanged.

Compression level
Use the drop-down list box to choose the degree of compression that you want MDaemon to apply to automatically compressed attachments. You can choose three levels of compression: minimum (fastest compression process with least compression), medium (default value), or maximum (slowest compression process but highest degree of compression).

Use fixed archive name: [archive name]
Click this checkbox and choose a name if you want the automatically compressed attachments to have a specific filename.

Compression exclusions

Exclude these attachments...
Click this button to specify files that you want to exclude from the automatic

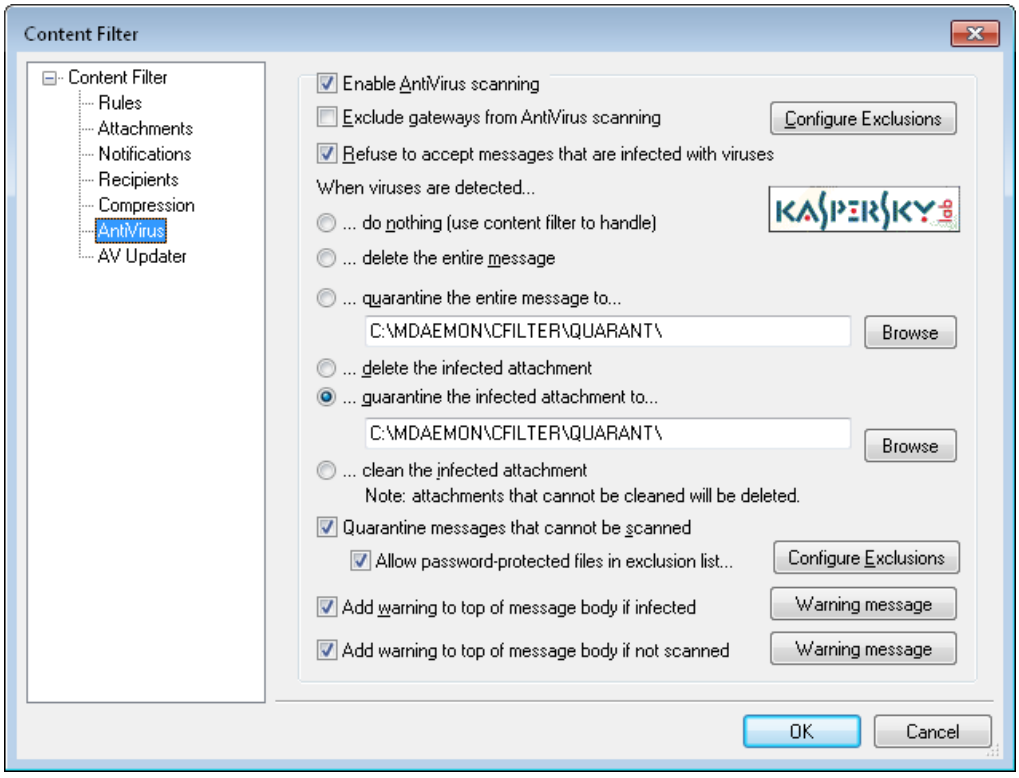
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

compression features. When a message attachment matches one of these filenames it will not be compressed, regardless of the compression settings. Wildcards are permitted in these entries. Therefore, you could specify "*.exe", for example, and all files ending with ".exe" would remain uncompressed.

Exclude these domains...
Click this button to specify recipient domains whose messages you wish to exclude from automatic compression. Messages bound for these domains will not have their file attachments compressed, regardless of your compression settings.

4.1.2 AntiVirus

4.1.2.1 AntiVirus



This screen (and the AV Updater 386 screen) will only be visible when you have installed SecurityPlus for MDaemon. To obtain SecurityPlus for MDaemon, visit www.altn.com.

Enable AntiVirus scanning

Click this checkbox to enable AntiVirus scanning of messages. When MDaemon receives a message with attachments, it will activate SecurityPlus for MDaemon and scan them for viruses before delivering the message to its final destination.

Exclude gateways from virus scanning
Click this checkbox if you want messages bound for one of MDaemon's domain

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

gateways to be excluded from virus scanning. This may be desirable for those who wish to leave the scanning of those messages to the domain's own mail server. For more information on domain gateways, see Gateway Manager 162.

Refuse to accept messages that are infected with viruses
Click this option is you wish to scan incoming messages for viruses during the SMTP session rather than after the session is concluded, and then reject those messages found to contain viruses. Because each incoming message is scanned before MDaemon officially accepts the message and concludes the session, the sending server is still responsible for it—the message hasn't technically been delivered yet. Thus the message can be rejected outright when a virus is found. Further, because the message was rejected, no further AntiVirus related actions listed on this dialog will be taken. No quarantine or cleaning procedures will be taken, and no notification messages will be sent. This can greatly reduce the number of infected messages and virus notification messages that you and your users receive.

The SMTP-(in) log will show the result of AV processing. The possible results you might see are:

- the message was scanned and found infected with a virus
- the message was scanned and no virus was found
- the message could not be scanned (usually because a ZIP or other type or attachment could not be opened/accessed)
- the message could not be scanned (it exceeds the max size limit)
- an error occurred during the scan

Configure Exclusions
Click the Configure Exclusions button to specify recipient addresses to exclude from virus scanning. Messages bound for these addresses will not be scanned for viruses by SecurityPlus for MDaemon. Wildcards are allowed in these addresses. You could therefore use this feature to exclude entire domains or specific mailboxes across all domains. For example, "*@example.com or "VirusArchive@*".

When viruses are detected...
Click one of the options in this section to designate the action that MDaemon will take when SecurityPlus for MDaemon detects a virus.

...do nothing (use content filter to handle)
Choose this option if you wish to take none of the above actions, and have set up content filter rules to take some alternative actions instead.

...delete the entire message
This option will delete the entire message rather than just the attachment when a virus is found. Because this deletes the whole message, the "*Add a warning...*" option doesn't apply. However, you can still send a notification message to the recipient by using the controls on the Notifications tab.

...quarantine the entire message to...
This option is like the "*Delete the entire message*" option above, but the message

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

will be quarantined in the specified location rather than deleted.

...delete the infected attachment
This option will delete the infected attachment. The message will still be delivered to the recipient but without the infected attachment. You can use the "*Add a warning...*" control on the bottom of this dialog to add text to the message informing the user that an infected attachment was deleted.

...quarantine the infected attachment to...
Choose this option and specify a location in the space provided if you want infected attachments to be quarantined to that location rather than deleted or cleaned. Like the "*Delete the infected attachment*" option, the message will still be delivered to the recipient but without the infected attachment.

...clean the infected attachment
When this option is chosen, SecurityPlus for MDaemon will attempt to clean (i.e. disable) the infected attachment. If the attachment cannot be cleaned, it will be deleted.

Quarantine messages that cannot be scanned
When this option is enabled, MDaemon will quarantine any messages it is unable to scan, such as some containing password-protected files.

Allow password-protected files in exclusion list...
Use this option if you wish to allow a message with a password-protected, non-scannable file to pass through antivirus scanner if the file name or type is in the exclusion list.

Configure Exclusions
Click this button to open and manage the file exclusion list. File name and types included on this list will not be scanned.

Add warning to top of message body if infected
When one of the "*...attachment*" options is chosen above, click this option if you want to add some warning text to the top of the previously infected message before it is delivered to the recipient. Thus you can inform the recipient that the attachment was stripped and why.

Warning message...
Click this button to display the warning text that will be added to messages when the "*Add a warning message...*" feature is used. After making any desired changes to the text, click "OK" to close the dialog and save the changes.

Add warning to top of message body if not scanned
When this option is enabled, MDaemon will add some warning text to the top of any message it is unable to scan.

Warning message...
Click this button to display the warning text that will be added to messages that cannot be scanned. After making any desired changes to the text, click "OK" to

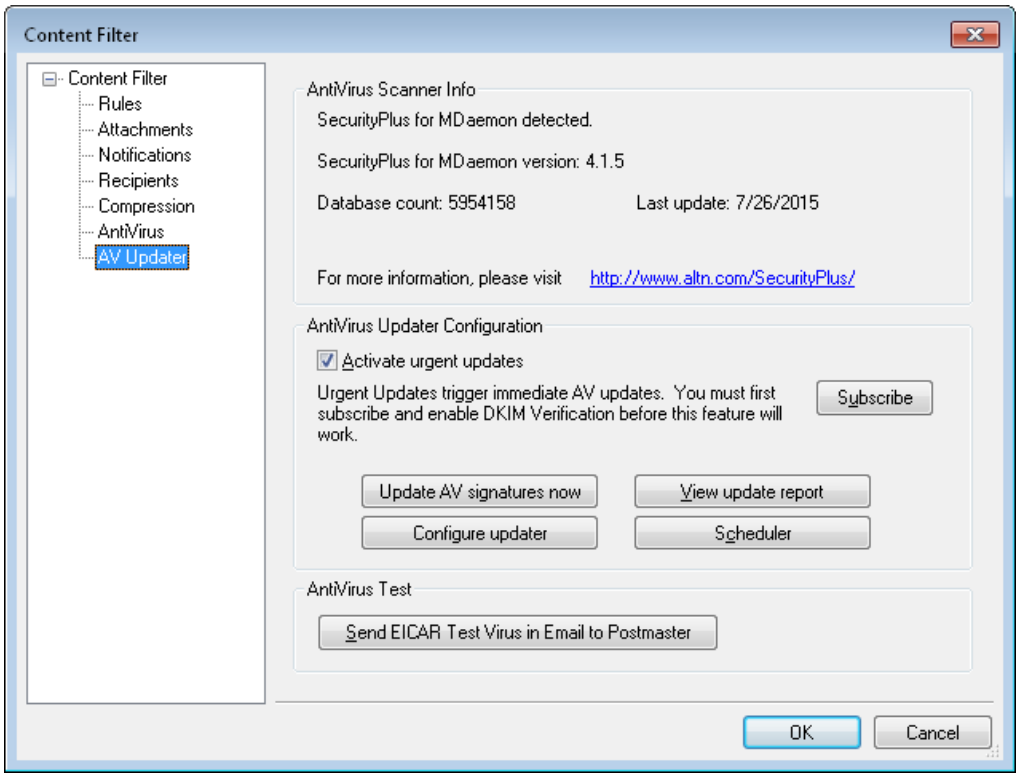
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

close the dialog and save the changes.

See:

AV Updater 386
Content Filter and AntiVirus 362

4.1.2.2 AV Updater



Use the controls on this screen to manually or automatically update SecurityPlus for MDaemon's virus definitions. There is a scheduler for automatic updating, a report viewer so that you can review when and which updates have been downloaded, and a test feature used for confirming that virus scanning is working properly.

AntiVirus Scanner Info

This section tells you whether SecurityPlus for MDaemon is installed and, if so, what version you are running. It also lists the date of your last virus definition update.

AntiVirus Updater Configuration

Activate urgent updates
Click this checkbox to activate the urgent updates feature. With this feature enabled, SecurityPlus will immediately connect to the update location and download the high-priority update whenever MDaemon receives an "Urgent Update" message.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

To receive these messages you must first subscribe to the "Urgent Updates" feature. See the *Subscribe* option below.

You must have the "*Verify...DKIM signatures*" option on the DKIM Verification 447 screen enabled to use this feature.

Subscribe
This button opens your default browser to Alt-N Technologies' Urgent Updates subscription page. On that page enter your domain name to subscribe your domain to the Urgent Updates mailing list. Whenever there is an urgent update to SecurityPlus for MDaemon's virus definitions, an email will be dispatched to the domain. When MDaemon receives the message, SecurityPlus will be updated immediately.

Update AV signatures now
Click this button to update the virus definitions manually. The updater will connect immediately after the button is pressed.

Configure updater
Click this button to open the Updater Configuration dialog 388. This dialog contains four tabs: Update URLs, Connection, Proxy, and Misc.

View update report
The SecurityPlus Log Viewer is opened by clicking the *View update report* button. The viewer lists the times, actions taken, and other information about each update.

Scheduler
Click this button to open MDaemon's Event Scheduler to the AntiVirus Updates 265 screen, used for scheduling checks for virus signature updates at specific times on specific days or at regular intervals. There is also an *Activate urgent updates* option on that screen that can be used to activate or deactivate Automatic Urgent Updates. That option is the same as the control of the same name described above.

AntiVirus Test

Send EICAR Test Virus in Email to Postmaster
Click this button to send a test message to the postmaster, with the EICAR virus file attached. This attachment is harmless – it is merely used for an antivirus test. By watching the Content Filter's log window on MDaemon's main interface you can see what MDaemon does with this message when it is received. For example, depending upon your settings, you might see a log excerpt that looks something like the following:

```
Mon 2008-02-25 18:14:49: Processing C:\MDAEMON\LOCALQ\md75000001128.msg
Mon 2008-02-25 18:14:49: > eicar.com (C:\MDaemon\CFilter\TEMP
\cf1772420862.att)
Mon 2008-02-25 18:14:49: > Message from: postmaster@example.com
Mon 2008-02-25 18:14:49: > Message to: postmaster@example.com
Mon 2008-02-25 18:14:49: > Message subject: EICAR Test Message
Mon 2008-02-25 18:14:49: > Message ID:
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

```
<MDAEMON10001200202251814.AA1447619@example.com>
Mon 2008-02-25 18:14:49: Performing viral scan...
Mon 2008-02-25 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 2008-02-25 18:14:50: > eicar.com was removed from message
Mon 2008-02-25 18:14:50: > eicar.com quarantined to C:\MDAEMON\CFILTER
\QUARANT\
Mon 2008-02-25 18:14:50: > Total attachments scanned    : 1 (including
multipart/alternatives)
Mon 2008-02-25 18:14:50: > Total attachments infected   : 1
Mon 2008-02-25 18:14:50: > Total attachments disinfected: 0
Mon 2008-02-25 18:14:50: > Total attachments removed    : 1
Mon 2008-02-25 18:14:50: > Total errors while scanning  : 0
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (sender)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (recipient)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2002-02-25 18:14:50: Processing complete (matched 0 of 12 active
rules)
```

See:

Updater Configuration Dialog 388
AntiVirus 383
Content Filter and AntiVirus 362

4.1.2.2.1 Updater Configuration Dialog

Click the *Configure updater* button on the AV Updater tab 386 to open the Updater Configuration dialog. It contains the following four tabs:

Update URLs
The Update URLs tab is used to designate the servers that SecurityPlus for MDaemon will check for updates. You can choose to let SecurityPlus manage these URLs automatically or manually enter them yourself.

Connection
The Connection tab is used to designate the Internet Connection Profile that SecurityPlus will use when connecting to the update sites. The "*Use Internet Settings from Control Panel*" option uses your default Internet settings. The "*Setup Internet settings manually*" option and subsequent controls can be used to manually choose a Connection Profile and designate its user name and password settings.

Proxy
The Proxy tab contains options for configuring any HTTP or FTP proxy settings that your current network configuration may require in order to connect to the update sites.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Misc
The Misc tab contains options governing updater logging. You can choose to log updater actions in a log file, and you can specify a maximum size for the file.

See:

AV Updater 386
AntiVirus 383
Content Filter and AntiVirus 362

4.2 Outbreak Protection

Outbreak Protection (OP) is a revolutionary real time anti-spam, anti-virus, and anti-phishing technology capable of proactively protecting an MDaemon email infrastructure automatically and within minutes of an outbreak. Included in SecurityPlus for MDaemon, Outbreak Protection requires SecurityPlus for MDaemon 3.0 or later and MDaemon PRO 9.5 or later, and it is accessible from MDaemon's Security menu (Security » Outbreak protection..., or Ctrl+Shift+1).

Outbreak Protection is completely content agnostic, meaning that it doesn't rely on strict lexical analysis of message content. Thus, it doesn't require heuristic rules, content filtering, or signature updates. Further, that means it is not fooled by the addition of seed text, clever spelling changes, social engineering tactics, language barriers, or differences in encoding techniques. Instead, OP relies on the mathematical analysis of message structure and message distribution characteristics over SMTP—it analyzes "patterns" associated with an email transmission and compares them to similar patterns collected from millions of email messages worldwide, which are sampled and compared in real time.

Because messages are being analyzed worldwide in real time, protection is provided within minutes—often seconds—of a new outbreak. For viruses, this level of protection is critical since it is often hours after an outbreak before a traditional antivirus vendor can verify and submit a virus signature update, and it can then be even longer before that update is put into production use. During that interval, servers without Outbreak Protection are vulnerable to that particular outbreak. Similarly, for spam messages it will often take time and effort to analyze the spam and create a safe filtering rule before it will be recognized by traditional heuristic and content based systems.

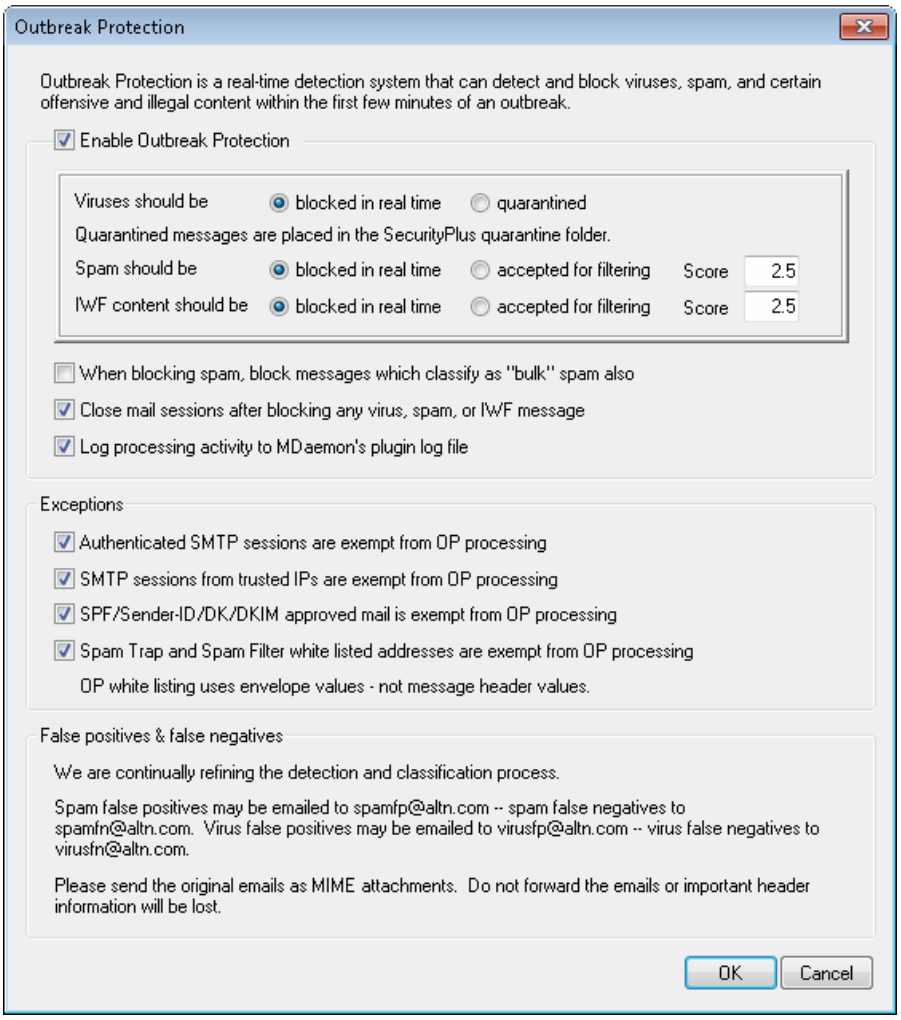
It is important to note, however, that the Outbreak Protection feature is not a replacement for traditional anti-virus, anti-spam, and anti-phishing techniques. In fact, OP provides another specialized layer of protection on top of the existing heuristics, signature, and content based tools found within SecurityPlus and MDaemon. Specifically, OP is designed to deal with large-scale outbreaks rather than old, unique, or specifically targeted messages that can be more readily caught by the traditional tools.

Outbreak Protection is based on CommTouch RPD and Zero-Hour technology. It works by extracting patterns from your

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

> incoming mail and comparing them to patterns taken from millions of internet email messages sampled daily from numerous sources all over the world. In no way is the actual content of any message ever transmitted, nor can the message content ever be derived from the extracted patterns.

For more on SecurityPlus and Outbreak Protection, see the remainder of this section and visit: www.altn.com.


Outbreak Protection
Outbreak Protection is a real-time detection system that can detect and block viruses, spam, and certain offensive and illegal content within the first few minutes of an outbreak.
Enable Outbreak Protection
Viruses should be
blocked in real time
quarantined
Quarantined messages are placed in the SecurityPlus quarantine folder.
Spam should be
blocked in real time
accepted for filtering
Score
2.5
IWF content should be
blocked in real time
accepted for filtering
Score
2.5
When blocking spam, block messages which classify as "bulk" spam also
Close mail sessions after blocking any virus, spam, or IWF message
Log processing activity to MDaemon's plugin log file
Exceptions
Authenticated SMTP sessions are exempt from OP processing
SMTP sessions from trusted IPs are exempt from OP processing
SPF/Sender-ID/DK/DKIM approved mail is exempt from OP processing
Spam Trap and Spam Filter white listed addresses are exempt from OP processing
OP white listing uses envelope values - not message header values.
False positives & false negatives
We are continually refining the detection and classification process.
Spam false positives may be emailed to spamfp@altn.com -- spam false negatives to spamfn@altn.com. Virus false positives may be emailed to virusfp@altn.com -- virus false negatives to virusfn@altn.com.
Please send the original emails as MIME attachments. Do not forward the emails or important header information will be lost.
OK
Cancel

Outbreak Protection

Enable Outbreak Protection

Click this checkbox to enable Outbreak Protection for your server. Incoming messages will be analyzed to see if they are part of an ongoing virus, spam, or phishing outbreak. The remaining options on this dialog are used to determine what will be done with messages found to be part of an outbreak, and to designate the senders that will be exempt from OP processing.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Viruses should be...

blocked in real time
Select this option if you wish to block messages during the SMTP process when they are determined to be part of a virus outbreak. These messages will not be quarantined or delivered to their intended recipients—they will be rejected by the server.

quarantined
Select this option if you wish to accept messages that OP determines are part of a virus outbreak. Although these messages will not be rejected by the server, they will be quarantined instead of delivered to their intended recipients. Quarantined messages are placed in the quarantine folder.

Spam should be...

blocked in real time
Select this option if you wish to block messages during the SMTP process when OP confirms that they are part of a spam outbreak. These messages will not be flagged as spam and delivered to their intended recipients—they will be rejected by the server. Messages classified by OP as "bulk" mail will not be blocked by this option unless you activate the *When blocking spam, block messages which classify as "bulk" spam also* option below. Messages classified as "bulk" by OP could simply be a part of certain very large mailing lists or other similar widely distributed content, so you may or may not consider those types of messages to be spam. For that reason, those types of messages generally shouldn't be scored negatively or blocked by OP.

accepted for filtering
Select this option if you wish to accept messages that OP confirms to be part of a spam outbreak, so that they can then be subjected to spam filtering and content filter processing. These messages will not be blocked by OP, but they will have their Spam Filter scores adjusted according to the *Score* option below.

When using the *accepted for filtering* option, OP will not directly cause a confirmed spam message to be blocked, but a message may still be blocked by MDaemon during the SMTP process if you have configured the Spam Filter to use the *SMTP rejects messages with scores greater than or equal to [xx]* option, located on the Spam Filter 402 screen.

For example, if the scoring option below caused a message's Spam Filter score to be 15.0, then the message would still be rejected as spam if you had also configured the Spam Filter's "*SMTP rejects...*" option to reject messages that have a score of 15.0 or greater.

Score
When using the *accepted for filtering* option above, this amount will be added to a message's Spam Filter score when OP confirms that the message is part of a spam outbreak.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

IWF Content

The following option applies to content identified by the Internet Watch Foundation (IWF) as referring to child abuse image sites (i.e. child pornography sites). It enables OP to use an integrated URL list provided by the IWF to detect and tag messages that refer to that content. The IWF operates an independent internet "hotline" for reporting potentially illegal online content, including child abuse content hosted anywhere in the world. They work in partnership with the police, governments, the wider online industry and the public to combat the availability of illegal online content. The Foundation's URL list is updated daily with new sites hosting child abuse images.

Many organizations have internal compliance rules governing the content of email sent or received by its employees, especially with regard to obscene or illegal material. In addition, many countries have outlawed the sending or receipt of such content. This feature can assist in your efforts to ensure compliance.

For more on the IWF, see:

http://www.iwf.org.uk/

IWF content should be...

blocked in real time
Choose this option if you wish to reject incoming messages during the SMTP process when they have IWF restricted content.

accepted for filtering
Choose this option if you wish to increase a message's Spam Filter score instead of rejecting it when it has IWF restricted content. The Spam Filter score will be increased by the amount specified in the *Score* option below.

Score
When the *accepted for filtering* option above is selected, this is the amount that will be added to a message's Spam Filter score when it contains IWF restricted content.

When blocking spam, block messages which classify as "bulk" spam also
Sometimes OP will identify certain messages that could be considered spam but aren't being sent from a known spammer or bot-net—as is sometimes the case with legitimate bulk mailings and newsletters. OP classifies these types of messages as "*Spam (bulk)*" rather than *"Spam (confirmed)*." Click this checkbox if you wish to apply OP's spam blocking features to "*Spam (bulk)*" mail as well. If this option is disabled, only messages classified as "*Spam (confirmed)*" will be affected by OP's spam blocking features above. Accepting this type of spam for later processing may be necessary for sites that want to receive bulk mailings but for some reason cannot white list the source or recipient.

Log processing activity to MDaemon's plugin log file
Enable this checkbox if you wish to log all OP processing activity into MDaemon's plugin log file.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Exceptions

Authenticated SMTP sessions are exempt from OP processing
When this option is enabled, authenticated SMTP sessions are exempt from OP processing. This means that messages sent during that session will not be subjected to Outbreak Protection checks.

SMTP sessions from trusted IPs are exempt from OP processing
Enable this option if you wish to exempt trusted IP addresses from Outbreak Protection—messages arriving from a server at a trusted IP address not be subjected to OP checks.

SPF/DKIM approved mail is exempt from OP processing
Click this checkbox if you wish to exempt a message from OP processing when the sending domain appears on the Approved List 474 and it is validated by SPF or DKIM.

Spam Trap and Spam Filter white listed addresses are exempt from OP processing
Click this option if you wish to exempt the Spam Honeypots 431 and Spam Filter white lists from Outbreak Protection. The "White List" applies to the recipient, or RCPT value given during the SMTP session. The "White List (from)" applies to the sender, or MAIL value given during the SMTP session. These operations are not based on message header values.

False Positives and False Negatives

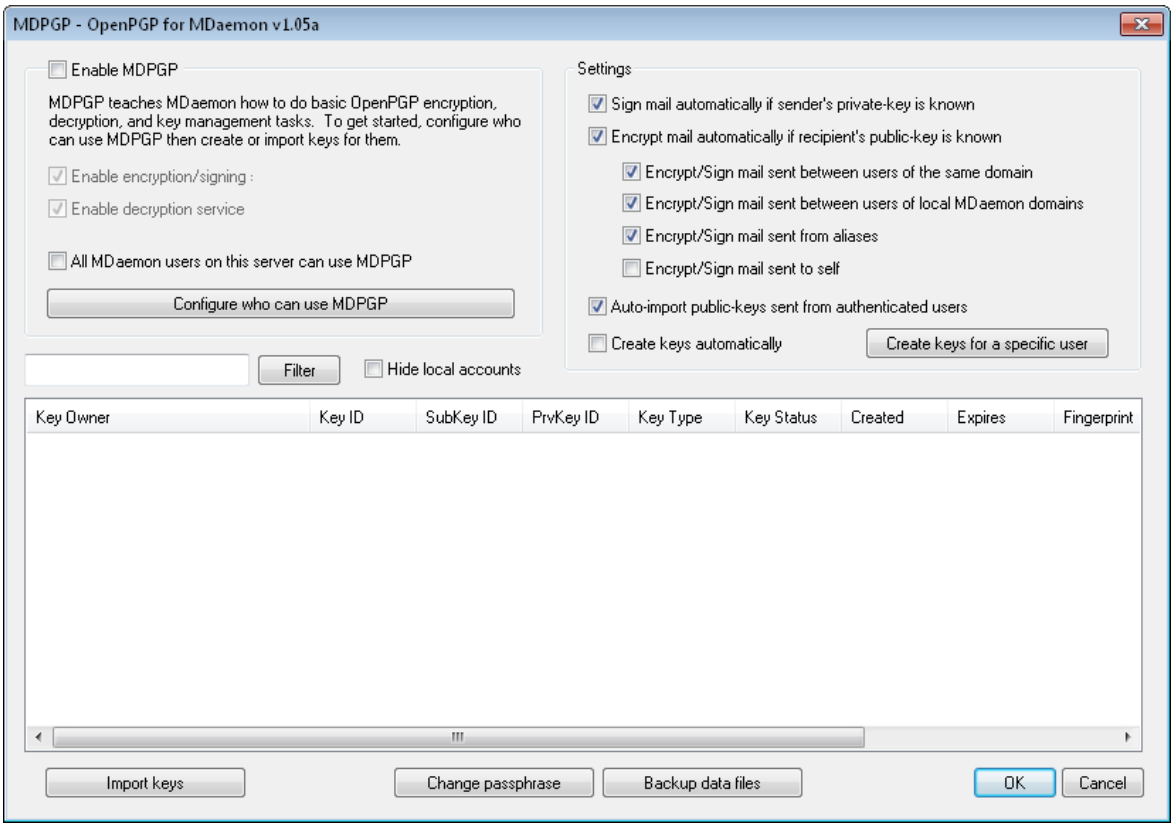
False positives, or classifying a legitimate message improperly as part of an outbreak, should rarely if ever happen. Should a false positive occur, however, you can send that message to us at **spamfp@altn.com** for spam/phishing false positives or **virusfp@altn.com** for virus false positives, so that we can use it to help refine and improve our detection and classification processes.

False negatives, or classifying a message as not part of an outbreak even though it is still spam or an attack, will happen more often than false positives. However, it worth noting that OP is not designed to catch all spam, virus attacks, and the like—it is simply one layer of protection that specifically targets outbreaks. Old messages, specifically targeted messages and the like, which are not part of a currently ongoing outbreak, might pass the OP check. Those sorts of messages should then be caught by the other AntiVirus and MDaemon features further down the processing chain. Should a false negative occur, however, you can send that message to us at **spamfn@altn.com** for spam/phishing false negatives or **virusfn@altn.com** for virus false negatives, so that we can use it to help refine and improve our detection and classification processes.

When sending improperly classified messages to us, the original email should be sent as a MIME email attachment rather than forwarded. Otherwise, headers and other information critical to the classification process will be lost.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.3 MDPGP


MDPGP - OpenPGP for MDaemon v1.05a
Enable MDPGP
MDPGP teaches MDaemon how to do basic OpenPGP encryption, decryption, and key management tasks. To get started, configure who can use MDPGP then create or import keys for them.
Enable encryption/signing :
Enable decryption service
All MDaemon users on this server can use MDPGP
Configure who can use MDPGP
Settings
Sign mail automatically if sender's private-key is known
Encrypt mail automatically if recipient's public-key is known
Encrypt/Sign mail sent between users of the same domain
Encrypt/Sign mail sent between users of local MDaemon domains
Encrypt/Sign mail sent from aliases
Encrypt/Sign mail sent to self
Auto-import public-keys sent from authenticated users
Create keys automatically
Create keys for a specific user
Filter
Hide local accounts
Key Owner
Key ID
SubKey ID
PrvKey ID
Key Type
Key Status
Created
Expires
Fingerprint
Import keys
Change passphrase
Backup data files
OK
Cancel

OpenPGP is an industry standard protocol for exchanging encrypted data, and there are a variety of OpenPGP plugins for email clients that make it possible for users to send and receive encrypted messages. MDPGP is MDaemon's integrated OpenPGP component that can provide encryption, decryption, and basic key management services for your users without requiring them to use an email client plugin.

MDPGP encrypts and decrypts emails using a public-key/private-key system. To do this, when you wish to use MDPGP to send a private and secure message to someone, MDPGP will encrypt that message using a "key" that you previously obtained from that person (i.e. his "public key") and imported into MDPGP. Conversely, if he wishes to send a private message to you, then he must encrypt the message using your public key, which he obtained from you. Giving the sender your public key is absolutely necessary, because without it he can't send you an OpenPGP encrypted message. Your unique public key must be used to encrypt the message because your unique private key is what MDPGP will use to decrypt the message when it arrives.

In order for MDPGP to manage signing, encrypting, and decrypting messages, it maintains two stores of keys (i.e. keyrings)—one for public keys and one for private keys. MDPGP can generate your users' keys automatically as needed, or you can create them manually for specific users. You can also import keys that were created elsewhere. Further, MDaemon can look for public keys attached to authenticated messages from local users, and then import those keys automatically. That way a user can request a public key from someone and then email that key to himself so that MDPGP will detect it and then import it into the public keyring. MDPGP will never store

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

multiple copies of the same key, but there can be multiple different keys for a single address. Finally, whenever a message arrives for an address that has a key in a keyring, MDPGP will sign, encrypt, or decrypt the message as needed, according to your settings. If an address has multiple keys, MDPGP will use the first one if encrypting the message, or try each one if decrypting it.

You can configure MDPGP's signing and encryption services to operate either automatically or manually. When set to operate automatically, MDPGP will automatically sign and encrypt messages whenever possible. When set to operate manually, MDPGP will only sign or encrypt a message when the sending user inserts a special command into the message's Subject. In any case messages will only be signed or encrypted (or decrypted) when the account has been given permission to use those services.

The OpenPGP specification is outlined in RFCs 4880 and 3156.

Enabling MDPGP

Enable MDPGP
MDPGP is disabled by default. Click this checkbox to enable it. Even when enabled, however, MDPGP will still not sign, encrypt, or decrypt any messages until you *Configure who can use MDPGP* (see below) and create or import keys into its keyrings.

Enable encryption/signing
When MDPGP is enabled, by default messages can be signed and encrypted when the required keys are in the keyring. Disable this option if you do not wish to allow MDPGP to sign or encrypt messages.

Messages can be signed without being encrypted, but any message that is encrypted by MDPGP will always be signed as well.

Enable decryption service
When MDPGP is enabled, by default incoming encrypted messages will be decrypted if the recipient's private key is known and his account is permitted to use the decryption service. Disable this option if you do not wish to allow MDPGP to decrypt any messages, for example if you want all of your users to handle their own decryption via an email client plugin. When disabled, any incoming encrypted message will be handled like a normal message and placed in the recipient's mailbox.

All MDaemon users on this server can use MDPGP
Enable this option if you wish to authorize all of your MDaemon user accounts to use MDPGP to sign, encrypt and/or decrypt messages, depending on the *Enable encryption/decryption* settings above. This option is disabled by default and not recommended. However, if you choose to enable this option, you can use the *Configure who can use MDPGP* option below to specifically exclude users whom you

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

do not wish to allow to use MDPGP.

Configure who can use MDPGP
Click this button to open the `rules.txt` file for configuring user permissions for MDPGP. Using this file you can specify who is allowed to sign messages, encrypt messages, and have messages decrypted. You can also specifically restrict users from these options. For example, you could use the rule "`+*@example.com`" to allow all `example.com` users to encrypt messages, but then add "`-frank@example.com`" to specifically prevent `frank@example.com` from being able to do so. See the text at the top of the `rules.txt` file for examples and instructions.

Rules.txt Notes and Syntax

- Only SMTP authenticated email from users of this MDaemon server are eligible for encryption service.
- If there is a conflict between the settings in `rules.txt` and the global "*All MDaemon users on this server can use MDPGP*" option, the `rules.txt` setting is used.
- Text after # on a line is ignored.
- Separate multiple email addresses on the same line with a space.
- Wildcards (* and ?) in email addresses are permitted.
- Even though MDPGP encrypted messages are **always** signed, granting encryption permission to a user doesn't also grant that user permission to sign unencrypted messages. In order to sign an unencrypted message the account must be given signing permission.
- Each email address must be prefixed with one of the following tags:

  + (plus) - address can use MDPGP encryption service.

  - (minus) - address **cannot** use MDPGP encryption service.

  ! (exclamation) - address can use MDPGP decryption service.

  ~ (tilde) - address **cannot** use MDPGP decryption service.

  ^ (caret) - address can use MDPGP signing service.

  = (equal) - address **cannot** use MDPGP signing service.

Examples:

`+*@*` — all users of all domains can encrypt.

`!*@*` — all users of all domains can decrypt.

`^*@*` — all users of all domains can sign.

`^*@example.com` — all users of example.com can sign.

`+frank@example.com ~frank@example.com` — the user can encrypt but not decrypt.

`+GROUP:EncryptingUsers` — members of MDaemon's `EncryptingUsers` group can encrypt

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

`^GROUP:Signers` — members of MDaemon's `Signers` group can sign

Encryption/Signing Modes

Automatic Mode

Use the Settings options to configure MDPGP to sign and encrypt messages automatically for accounts permitted to do so. When an account sends an authenticated message and MDPGP knows the required key, the message will be signed or encrypted according to the settings below.

The special Subject codes outlined in the Manual Mode section below always take precedence over the Automatic Mode options. Therefore if one of these options is disabled, an account that is permitted to sign or encrypt messages can still manually cause a message to be signed or encrypted by using one of the codes.

Settings

Sign mail automatically if sender's private key is known
By default, if an account is allowed to sign messages, MDPGP will sign them automatically if the sending account's private key is known. Disable this option if you do not wish to sign them automatically; messages can still be signed manually by using the special codes outlined in the Manual Mode section below.

Encrypt mail automatically if recipient's public key is known
By default, if an account is allowed to encrypt messages, MDPGP will encrypt them automatically if the recipient's public key is known. Disable this option if you do not wish to encrypt them automatically; messages can still be encrypted manually by using the special codes outlined in the Manual Mode section below.

Encrypt/Sign mail between users of the same domain
When MDPGP is set to encrypt or sign messages automatically, this option causes MDPGP to do this even when messages are sent between users of the same domain, provided the required keys are known. This option is enabled by default.

Encrypt/Sign mail between users of local MDaemon domains
When MDPGP is set to encrypt or sign messages automatically, this option causes MDPGP to do this even when messages are being sent between users of local MDaemon domains, provided the required keys are known. For example, if your MDaemon domains include "example.com" and "example.net," then messages sent between those domains' users will be automatically encrypted or signed. This option is enabled by default.

Encrypt/Sign mail sent from aliases
When MDPGP is set to encrypt or sign messages automatically, this option causes MDPGP to do this even when the sending account is using an alias. For example, if frank.thomas@example.com is sending a message from his alias

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

frank@example.com, this option causes the message to be signed or encrypted whenever possible. If this option is disabled then messages sent from an account's alias will not be encrypted or signed automatically. This option is enabled by default.

Encrypt/Sign mail sent to self
When MDPGP is set to encrypt or sign messages automatically, this option would cause MDPGP to do this even when an account is sending a message to itself (e.g. frank@example.com sending to frank@example.com). If the account has permission to use both encryption and decryption then this would effectively cause MDPGP to accept the message, encrypt it, and then immediately decrypt it and place it in the same user's mailbox. If, however, the account wasn't configured for decryption, then this would cause the message to be encrypted and then placed in the same user's mailbox still encrypted. This option is disabled by default.

Manual Mode

When you have disabled the *Sign mail automatically...* and *Encrypt mail automatically...* options outlined above, you are using MDPGP in Manual Mode. MDPGP will not sign or encrypt any messages except those that are authenticated and have one of the following codes in the message's Subject header:

--pgps Sign this message if possible. Code can be placed at the beginning or end of the Subject.

--pgpe Encrypt this message if possible. Code can be placed at the beginning or end of the Subject.

--pgpx The message **MUST** be encrypted. If it cannot be encrypted (e.g. because the recipient's key isn't known) then do not deliver it; the message will be bounced/returned to the sender. Code can be placed at the beginning or end of the Subject.

--pgpk Send me my public key. The user places this code at the beginning of the Subject and sends the message to himself. MDPGP will then email the user his public key.

--pgpk<Email> Send me this address' public key. The user places this code at the beginning of the Subject and sends the message to himself. MDPGP will then email the user the address' public key.

Example:

```
Subject: --pgpk<frank@example.com>
```

Key Management

Public and private keys are managed using the options on the bottom half of the MDPGP dialog. There is an entry for each key, and you can right-click any entry to export the key, delete it, or enable/disable it. When you click **Export Key** it will be saved to the `\MDaemon\Pem\_mdpgp\exports\` folder and you can optionally email the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

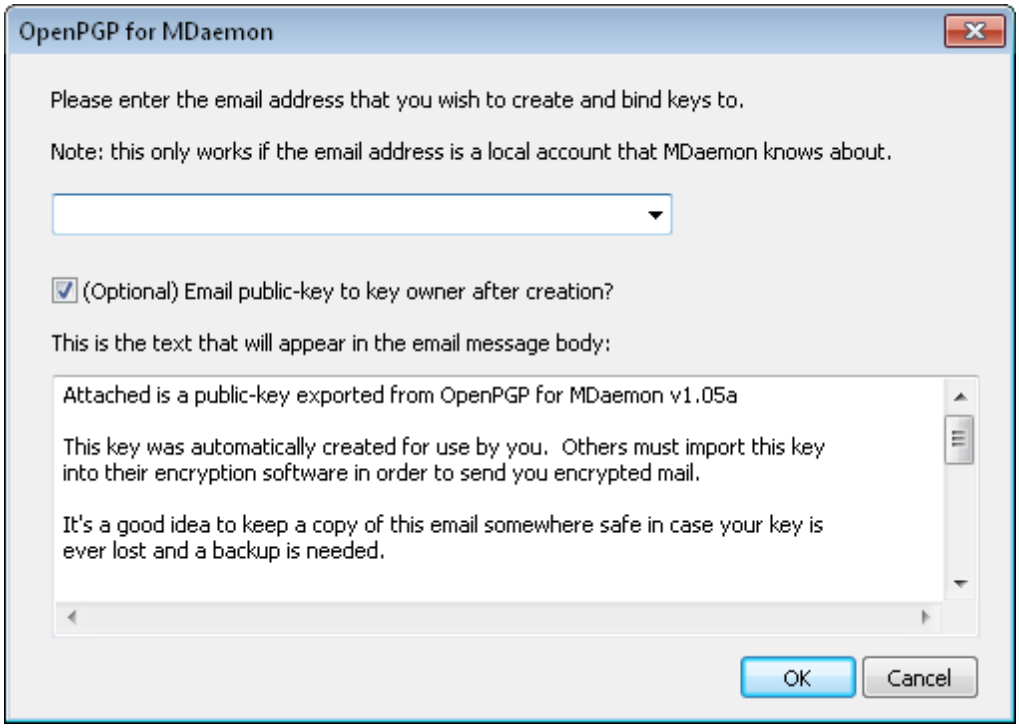
public key to an email address. "Hide local accounts" and "Filter" options are provided to help you locate certain addresses or groups.

Auto-import public keys sent from authenticated users
By default, when an authenticated user sends an email message with a public key in ASCII armored format attached, MDPGP will import that public key into the keyring. This is a simple way for a user to get a contact's public key into MDPGP, by emailing the public key to himself as an attachment. Disable this option if you do not wish to auto-import public keys.

Create keys automatically
Enable this option if you want MDPGP to create a public/private key pair automatically for each MDaemon user. Rather than generate them all at once, however, MDPGP will create them over time, creating each user's key pair the next time a message is processed for that user. This option is disabled by default to conserve resources and avoid needlessly generating keys for accounts that may never use MDPGP.

Create keys for a specific user
To manually generate a key pair for an account:

1. Click **Create keys for a specific user**.
2. Select the account from the drop-down list.
3. **Optional:** Check the box **Email public key to key owner...** if you wish to send the key to the user as an email attachment.
4. Click **Ok**.


OpenPGP for MDaemon
Please enter the email address that you wish to create and bind keys to.
Note: this only works if the email address is a local account that MDaemon knows about.
(Optional) Email public-key to key owner after creation?
This is the text that will appear in the email message body:
Attached is a public-key exported from OpenPGP for MDaemon v1.05a
This key was automatically created for use by you. Others must import this key into their encryption software in order to send you encrypted mail.
It's a good idea to keep a copy of this email somewhere safe in case your key is ever lost and a backup is needed.
OK
Cancel

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Import keys
If you wish to import a key file into MDPGP manually, click this button, locate the key file, and click **Open**. When importing a private key file, you do not need to import the corresponding public key, as it is included in the private key. If you are importing a private key protected by a passphrase then MDPGP will prompt you to enter the passphrase. Without the passphrase you cannot import the private key. After importing a private key, MDaemon will change that key's passphrase to whichever passphrase MDPGP is currently using.

Change passphrase
Private keys are protected at all times by a passphrase. When attempting to import a private key, you must enter its passphrase. When exporting a private key, that exported key will still be protected by the passphrase, and it cannot be used or imported elsewhere without it. MDPGP's default passphrase is **MDaemon**. For security reasons you should change this passphrase after you begin using MDPGP, because until you do so, every key created by or successfully imported into MDPGP will have its passphrase set (or changed) to **MDaemon**. You can change the passphrase at any time by clicking **Change passphrase** on the MDPGP screen. When you change the passphrase, every private key on the keyring is updated to the new passphrase.

Backup data files
Click this button to make a backup of your current `Keyring.private` and `Keyring.public` keyring files. By default the backup files will be copied to: "`\MDaemon\Pem\_mdpgp\backups`" and have a date and `.bak` extension appended to the filenames.

- Forwarded messages are not encrypted.
- Autoresponder messages are not encrypted.
- Key servers and key revocation are not supported.
- The Content Filter encrypt action does not act on messages already encrypted, and the encrypt and decrypt actions are subject to all MDPGP configuration requirements.
- The drop-down lists that display MDaemon accounts show the first 500 accounts by default. You can set `MaxUsersShown=0` in `plugins.dat` to view all accounts. This may take longer to load for very large user lists.
- `MDPGPUtil.exe` is a tool that can encrypt and decrypt via command line options. Run MDPGPUtil with no arguments from a command line shell for help.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.4 Spam Filter

4.4.1 Spam Filter

The Spam Filter is one of the main features in MDaemon's extensive suite of spam prevention tools. It incorporates heuristics to examine incoming email messages in order to compute a "score" based on a complex system of rules. The score is then used to determine the likelihood of a message being spam, and certain actions can be taken based on that score — you can refuse the message, flag it as possible spam, and so on.

Addresses can be white or black listed, or designated as completely exempt from Spam Filter examination. You can have a spam report inserted into messages, showing their spam scores and how those scores were achieved, or you can generate the report as a separate email and have the original spam message included with it as an attachment. Further, you can even use Bayesian 405 learning to help the Spam Filter learn to identify spam more accurately over time, thus increasing its reliability.

Finally, by examining many thousands of known spam messages, the rules have been optimized over time and are very reliable in detecting the fingerprint of a spam message. You can, however, customize or add new rules by editing the Spam Filter's configuration files to meet your specific needs.

MDaemon's Spam Filter uses an integrated, popular open-source heuristic technology. The homepage for the open-source project is:

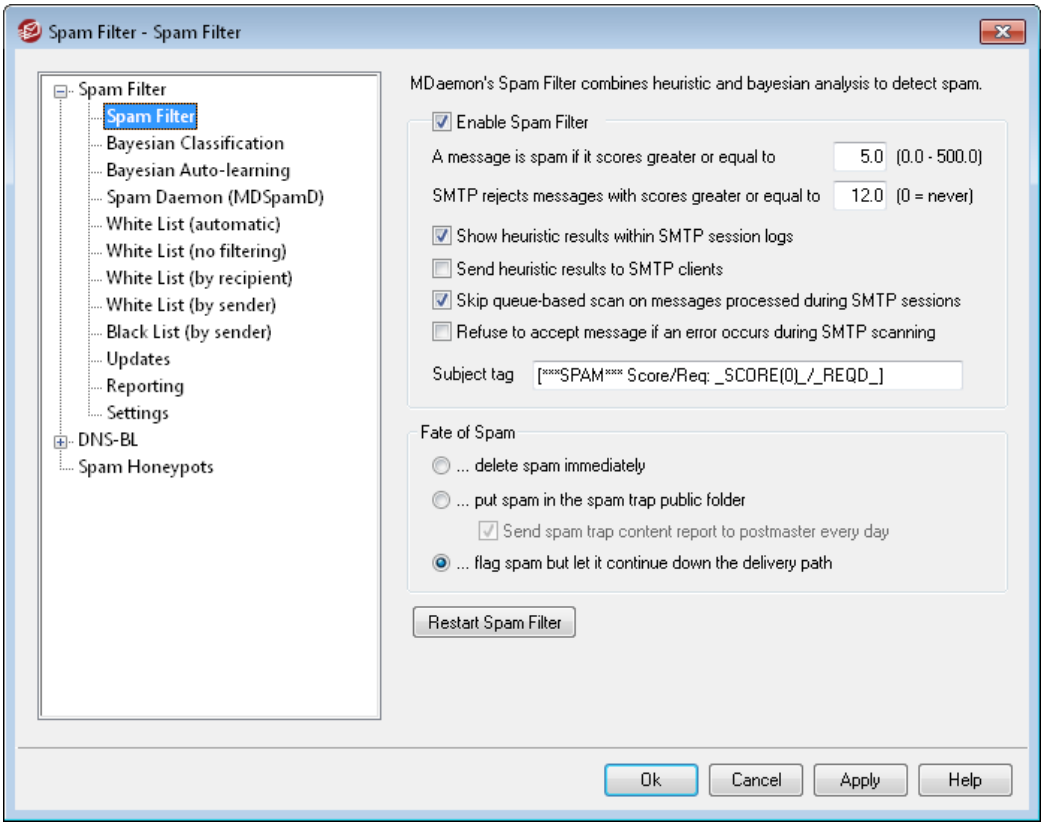
```
http://www.spamassassin.org
```

See:

Spam Filter 402
DNS Black Lists 425

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.4.1.1 Spam Filter


Spam Filter - Spam Filter
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
MDaemon's Spam Filter combines heuristic and bayesian analysis to detect spam.
Enable Spam Filter
A message is spam if it scores greater or equal to
5.0
(0.0 - 500.0)
SMTP rejects messages with scores greater or equal to
12.0
(0 = never)
Show heuristic results within SMTP session logs
Send heuristic results to SMTP clients
Skip queue-based scan on messages processed during SMTP sessions
Refuse to accept message if an error occurs during SMTP scanning
Subject tag
[***SPAM*** Score/Req: _SCORE(0)_/_REQD_]
Fate of Spam
... delete spam immediately
... put spam in the spam trap public folder
Send spam trap content report to postmaster every day
... flag spam but let it continue down the delivery path
Restart Spam Filter
Ok
Cancel
Apply
Help

Enable Spam Filter

Check this box to activate the heuristic message-scoring, spam filtering system. None of the other Spam Filter options on this screen will be available until this option is enabled.

A message is spam if its score is greater or equal to [XX] (0.0-500.0)
The value that you specify here is the required spam threshold that MDaemon will compare to each message's spam score. Any message with a spam score greater than or equal to this amount will be considered spam, and then the appropriate actions will be taken based on your other Spam Filter settings.

SMTP rejects messages with scores greater or equal to XX (0=never)
Use this option to designate a spam score rejection threshold. When a message's spam score is greater than or equal to this score it will be rejected completely rather than proceed through the rest of the options and possibly be delivered. The value of this option should always be greater than the value of the "*A message is spam if its score...*" option above. Otherwise, a message would never be considered spam and have the rest of the Spam Filter's options applied to it—it would simply be rejected during delivery. Use "0" in this option if wish to disable scanning during the SMTP process, and if you do not want MDaemon to reject any messages regardless of their scores. If SMTP scanning is disabled then a queue-based scan will still be performed on the messages after they are accepted. The default setting for this option is "12.0".

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Example,

If you have the spam score threshold set to 5.0 and the rejection threshold set to 10.0, then any message with a spam score that is greater than or equal to 5.0 but less than 10.0 will be considered spam and handled according to the rest of your Spam Filter settings. Any message with a spam score greater than or equal to 10.0 will be rejected by MDaemon during the delivery process.

You should monitor the spam filter's performance over time and refine both the spam and rejection thresholds to suit your need. For most people, however, a spam score threshold of 5.0 will catch most spam, with relatively few false negatives (spam that slips through unrecognized) and rarely any false positives (messages flagged as spam that are not). A rejection threshold of 10-15 will cause only messages that are almost certainly spam to be rejected. It is extremely rare that a legitimate message will have a score that high. The default rejection threshold is 12.

Show heuristic results within SMTP session logs
Click this option to log the results of heuristic processing during SMTP sessions to the SMTP session logs 116.

Send heuristic results to SMTP clients
Click this option to display heuristic processing results inline with SMTP session transcripts. This option is not available when you have your Spam Score rejection threshold set to "0", meaning that spam will never be rejected because of its score. For more information see, "*SMTP rejects messages with scores greater or equal to XX (0=never)*" above.

Skip queue-based scan on messages processed during SMTP sessions
By default, MDaemon scans messages during the SMTP session to determine whether or not they should be rejected for having a spam score above the rejection threshold. For messages that are accepted MDaemon will then perform another, queue-based, scan and treat the messages accordingly, based on their scores and your spam filter configuration. Click this option if you want MDaemon to omit the queue-based scan and treat the results of the initial Spam Filter scan as definitive. This can potentially significantly decrease CPU usage and increase the efficiency of the AntiSpam system. However, only the default SpamAssassin headers will be added to messages when the queue-based scan is omitted. If you have made any changes to the default SpamAssassin headers or specified custom headers in your `local.cf` file, those changes and additions will be ignored.

Refuse to accept message if an error occurs during SMTP scanning
Click this option if you want a message to be refused when an error is encountered while it is being scanned during the SMTP process.

Subject tag
This tag will be inserted at the beginning of the Subject header of all messages that meet or exceed the required spam score threshold. It can contain information about

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

the spam score, and you can use your IMAP message filters to search for it and filter the message accordingly (assuming that you have the Spam Filter configured to continue delivering spam messages). This is a simple method for automatically routing spam messages to a designated "spam" folder. If you want to dynamically insert the message's spam score and the value of the required spam threshold then use the tag "_HITS_" for the message's score and "_REQD_" for the required threshold. Alternatively, you can use "_SCORE(0)_" instead of "_HITS_"— this will insert a leading zero into lower scores, which can help ensure the proper sort-order when sorting messages by subject in some email clients.

Example,

A subject tag set to: `***SPAM*** Score/Req: _HITS_/_REQD_ -`
will cause a spam message with a score of 6.2 and the subject: "Hey, here's some spam!" to be changed to "***SPAM*** Score/Req: 6.2/5.0 – Hey, here's some spam!"

If "_SCORE(0)_" is substituted for "_HITS_" then it would be changed to "***SPAM*** Score/Req: 06.2/5.0 – Hey, here's some spam!"

If you do not wish to alter the subject header then leave this option blank. No subject tag will be inserted.

This option is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. The Subject tag configuration will be determined by the other server's settings. See: Spam Daemon, for more information.

Fate of Spam

The Spam Filter will perform the action chosen below if a message's spam score is greater than or equal to the spam score specified above.

...delete spam immediately
Choose this option if you wish simply to delete any incoming message whose spam score is equal to or exceeds the designated limit.

...put spam in the spam trap public folder
Choose this option if you want to flag messages as spam and then move them to the spam public folder rather than allow them to be delivered.

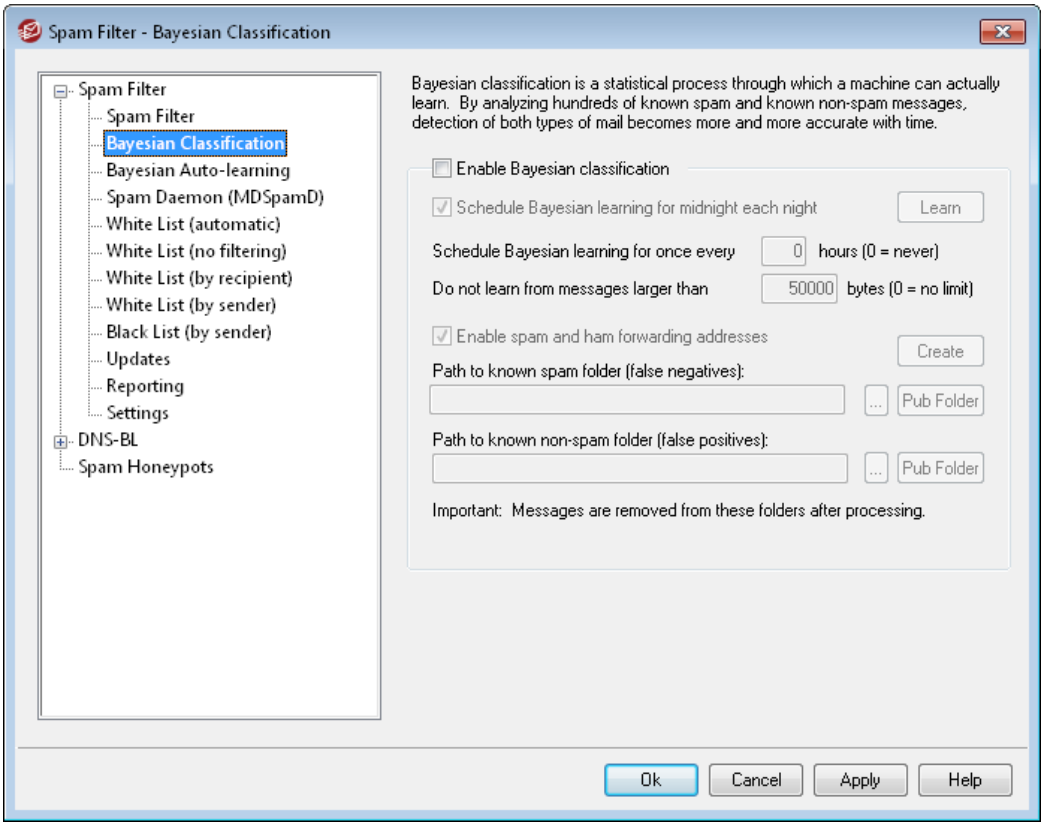
Send spam trap content report to postmaster every day
When using the *...put spam in the spam trap public folder* option above, check this box if you would like the postmaster to receive a daily message with a summary of the folder's contents.

...flag spam but let it continue down the delivery path
Choose this option if you want to go ahead and deliver each spam message to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

its intended recipient, but flag it as spam by inserting various spam headers and/or tags designated above and on the Reporting 421 screen. This is the default option, which allows users to take advantage of options such as filtering mail into a spam folder for their review and thus avoid losing messages that may be erroneously labeled as spam (i.e. false positives).

4.4.1.2 Bayesian Classification


Spam Filter - Bayesian Classification
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
Bayesian classification is a statistical process through which a machine can actually learn. By analyzing hundreds of known spam and known non-spam messages, detection of both types of mail becomes more and more accurate with time.
Enable Bayesian classification
Schedule Bayesian learning for midnight each night
Learn
Schedule Bayesian learning for once every
0
hours (0 = never)
Do not learn from messages larger than
50000
bytes (0 = no limit)
Enable spam and ham forwarding addresses
Create
Path to known spam folder (false negatives):
Pub Folder
Path to known non-spam folder (false positives):
Pub Folder
Important: Messages are removed from these folders after processing.
Ok
Cancel
Apply
Help

Bayesian Classification is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. All Bayesian learning will be performed on the other server. See the Spam Daemon 411 screen for more information.

The Spam Filter supports Bayesian learning, which is a statistical process that can optionally be used to analyze spam and non-spam messages in order to increase the reliability of spam recognition over time. You can designate a folder for spam messages and non-spam message that will can be scanned manually or automatically at regular

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

intervals. All of the messages in those folders will be analyzed and indexed so that new messages can be compared to them statistically in order to determine the likelihood that they are spam. The Spam Filter can then increase or decrease a message's spam score based upon the results of its Bayesian comparison.

The Spam Filter will not apply a Bayesian classification to messages until a Bayesian analysis has been performed on the number of spam and non-spam messages designated on the Bayesian Auto-learning 409 screen. This is necessary in order for the Spam Filter to have a sufficient pool of statistics to draw from when making the Bayesian comparison. Once you have given the system these messages to analyze, it will be sufficiently equipped to begin applying the results of a Bayesian comparison to each incoming message's spam score. By continuing to analyze even more messages the Bayesian classifications will become more accurate over time.

Bayesian Classification

Enable Bayesian classification
Click this check box if you want each message's spam score to be adjusted based on a comparison to the currently known Bayesian statistics.

Schedule Bayesian learning for midnight each night
When this option is active, once each day at midnight the Spam Filter will analyze and then delete all messages contained in the spam and non-spam folders specified below. If you wish to schedule Bayesian learning for some other time interval then clear this option and use the *Schedule Bayesian learning for once every XX hours* option below. If you do not wish Bayesian learning to ever occur automatically, then clear this option and specify "0" hours in the option below.

Schedule Bayesian learning for once every XX hours (0=never)
If you wish Bayesian learning to occur at some time interval other than once each night at midnight, then clear the above option and specify a number of hours in this option instead. Each time that number of hours has elapsed, the Spam Filter will analyze and then delete all messages contained in the spam and non-spam folders specified below. If you do not wish Bayesian learning to ever occur automatically, then clear the above option and specify "0" hours in this option.

If for some reason you do not want the messages to be deleted after they are analyzed then you can prevent that by copying `LEARN.BAT` to `MYLEARN.BAT` in the `\MDaemon\App\` subfolder and then deleting the two lines that begin with "`if exist`" near the bottom in that file. When the `MYLEARN.BAT` file is present in that folder MDaemon will use it instead of `LEARN.BAT`. See `SA-Learn.txt` in your `\MDaemon\SpamAssassin\` subfolder for more information.

For more detailed information on heuristic spam filtering

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

technology and Bayesian learning, visit:

http://www.spamassassin.org/doc/sa-learn.html

Don't learn from messages larger than XX bytes (0=no limit)
Use this option to designate a maximum message size for Bayesian analysis. Messages larger this value will not be analyzed. Specify "0" in this option if you do not wish to implement any size restriction.

Learn
Click this button to initiate a manual Bayesian analysis of the designated folders rather than waiting for the automatic analysis.

Enable spam and ham forwarding addresses
Click this check box if you wish to allow users to forward spam and non-spam (ham) messages to designated addresses so that the Bayesian system can learn from them. The default addresses that MDaemon will use are "SpamLearn@<domain>" and "HamLearn@<domain>". Messages sent to these addresses must be received via SMTP from a session that is authenticated using SMTP AUTH. Further, MDaemon expects the messages to be forwarded to the above addresses as attachments of type "message/rfc822". Any message of another type that is sent to these email addresses will not be processed.

You can change the addresses MDaemon uses by adding the following key to the CFilter.INI file:

```
[SpamFilter]
SpamLearnAddress=MySpamLearnAddress@
HamLearnAddress=MyNonSpamLearnAddress@
```

Note: the last character of these values must be "@".

Create
Click this button to create spam and non-spam Public IMAP Folders 84 automatically, and to configure MDaemon to use them. The following folders will be created:

\Bayesian Learning.IMAP\	Root IMAP folder
\Bayesian Learning.IMAP\Spam.IMAP\	This folder is for false negatives (spam that doesn't score high enough to get flagged as such).
\Bayesian Learning.IMAP\Non-Spam.IMAP\	This folder is for false positives (non-spam messages that erroneously score high enough to get flagged as spam).

By default, access permission to these folders is only granted to local users of local domains and is limited to Lookup and Insert. The postmaster's default permissions are Lookup, Read, Insert, and Delete.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Path to known spam folder (false negatives):
This is the path to the folder that will be used for Bayesian analysis of known spam messages. Only copy messages to this folder which you consider to be spam. You should not automate the process of copying messages to this folder unless doing so via the Bayesian Auto-learning 409 or Spam Honeypots 431 options. Automating this process by some other means could potentially cause non-spam messages to be analyzed as spam, which would decrease the reliability of the Bayesian statistics.

Path to known non-spam folder (false positives):
This is the path to the folder that will be used for Bayesian analysis of messages that are definitely **not** spam. Only messages that you do **not** consider to be spam should be copied to this folder. You should not automate the process of copying messages to this folder unless doing so via the Bayesian Auto-learning 409 options. Automating this process by some other means could potentially cause spam messages to be analyzed as non-spam, which would decrease the reliability of the Bayesian statistics.

Pub Folder
Click one of these buttons to designate one of your existing Public Folders as the Bayesian directory. This is an easy way for your users to place their messages incorrectly categorized as spam or non-spam into your Bayesian directories for analysis. Note, however, that giving access to more people increases the likelihood that some messages will be put into the wrong folders thus skewing the statistics and decreasing reliability.

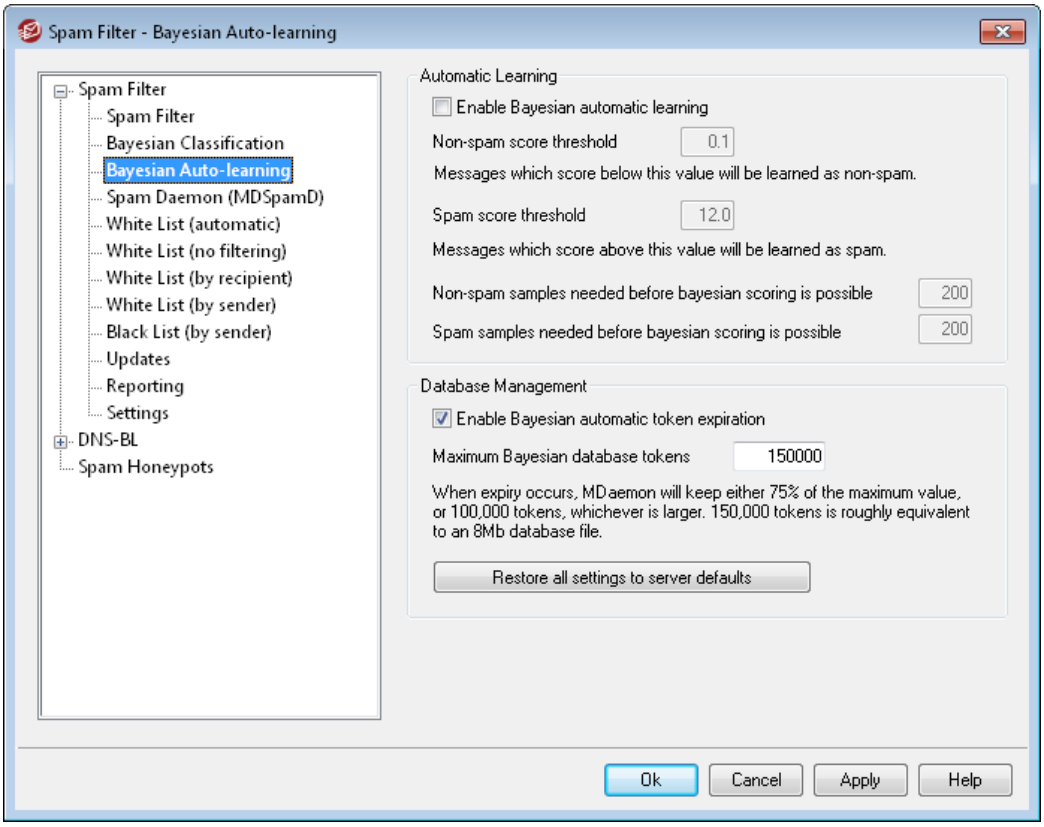
If you rename a Public folder via a mail client, Windows Explorer, or some other means, then you must manually reset this path to the appropriate new folder name. If you rename a folder but do not change its path here, the Spam Filter will continue to use this path for the Bayesian folder instead of the new one.

See:

Bayesian Auto-learning 409
Spam Honeypots 431

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.4.1.3 Bayesian Auto-learning



Bayesian Auto-learning is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. All Bayesian learning will be performed on the other server. See the Spam Daemon 411 screen for more information.

Automatic Learning

Enable Bayesian automatic learning
With automatic Bayesian learning you can designate spam and non-spam scoring thresholds, which make it possible for the Bayesian learning system to learn from messages automatically rather than requiring you to manually place those messages in the spam and non-spam folders. Any message scoring below the non-spam threshold will be treated by automatic learning as non-spam, and any message scoring above the spam threshold will be treated as spam. With automatic learning, old expired tokens that are removed from the database (see *Database Management* below) can be replaced automatically. This prevents the need for manual retraining to recover expired tokens. Automatic Learning can be useful and beneficial as long if you are careful in setting your thresholds, to avoid placing improperly classified

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

messages in the folders.

Non-spam score threshold
Messages with a spam score below this value will be treated as non-spam messages by the Bayesian Classification system.

Spam score threshold
Messages with a spam score above this value will be treated as spam messages by the Bayesian Classification system.

Non-spam samples needed before Bayesian scoring is possible
The Spam Filter will not apply a Bayesian classification to messages until this number of non-spam messages (and spam messages specified in the next option) has been analyzed by the Bayesian system. This is necessary in order for the Spam Filter to have a sufficient pool of statistics to draw from when making the Bayesian comparison. Once you have given the system these messages to analyze, it will be sufficiently equipped to begin applying the results of a Bayesian comparison to each incoming message's spam score. By continuing to analyze even more messages the Bayesian classifications will become more accurate over time.

Spam samples needed before Bayesian scoring is possible
Just as the previous option applies to non-spam messages, this option is for designating the number of *spam* messages that must be analyzed before the Spam Filter will begin applying a Bayesian classification to messages.

Database Management

Enable Bayesian automatic token expiration
Click this option if you want the Bayesian system to automatically expire database tokens whenever the number of tokens specified below is reached. Setting a token limit can prevent your Bayesian database from getting excessively large.

Maximum Bayesian database tokens
This is the maximum number of Bayesian database tokens allowed. When this number of tokens is reached, the Bayesian system removes the oldest, reducing the number to 75% of this value, or to 100,000 tokens, whichever is higher. The number of tokens will never fall below the larger of those two values regardless of how many tokens are expired. Note: 150,000 database tokens is approximately 8Mb.

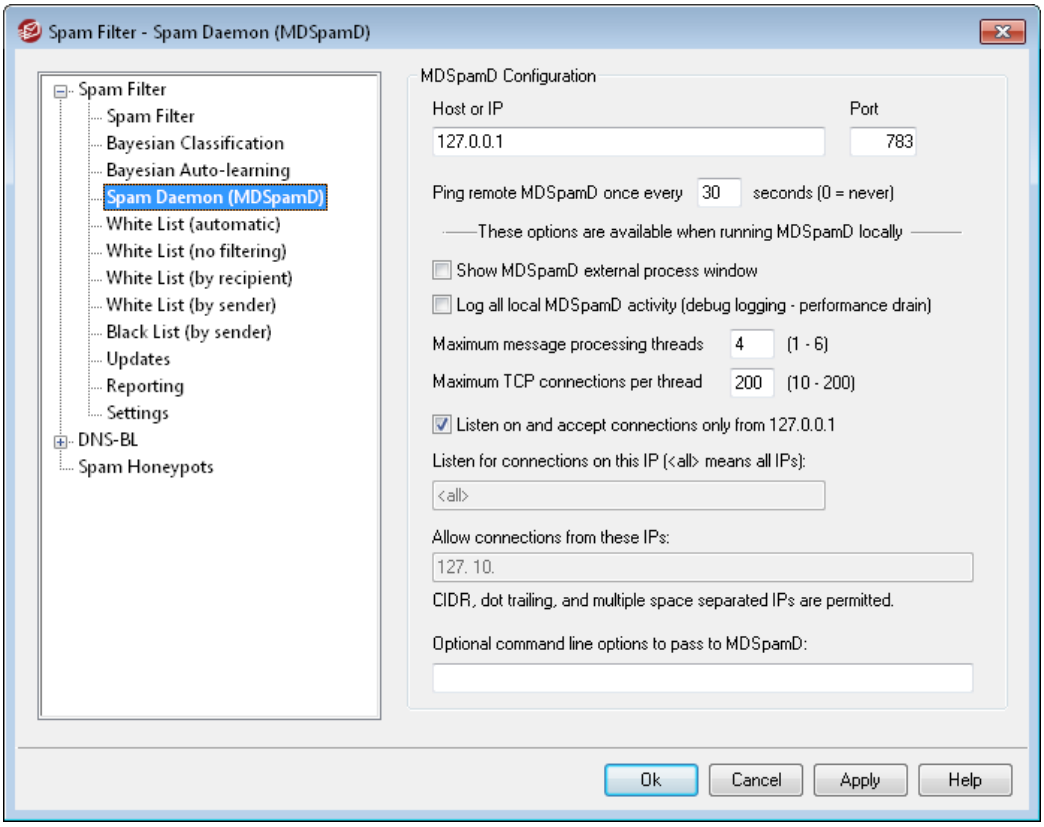
Restore all settings to server defaults
Click this button to restore all of the Bayesian advanced options to their default values.

See:

Bayesian Classification 405
Spam Honeypots 431

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.4.1.4 Spam Daemon (MDSpamD)


Spam Filter - Spam Daemon (MDSpamD)
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
MDSpamD Configuration
Host or IP
127.0.0.1
Port
783
Ping remote MDSpamD once every 30 seconds (0 = never)
These options are available when running MDSpamD locally
Show MDSpamD external process window
Log all local MDSpamD activity (debug logging - performance drain)
Maximum message processing threads 4 (1 - 6)
Maximum TCP connections per thread 200 (10 - 200)
Listen on and accept connections only from 127.0.0.1
Listen for connections on this IP (<all> means all IPs):
<all>
Allow connections from these IPs:
127. 10.
CIDR, dot trailing, and multiple space separated IPs are permitted.
Optional command line options to pass to MDSpamD:
Ok
Cancel
Apply
Help

MDaemon's spam filtering system runs as a separate daemon—the MDaemon Spam Daemon (MDSpamD), which is fed messages via TCP/IP for scanning. This greatly increases the Spam Filter's performance and makes it possible for you to run MDSpamD locally, on a separate computer, or have MDaemon use another MDSpamD (or any other Spam Daemon enabled product) running at some other location. By default MDSpamD runs locally and receives messages on port 783 at 127.0.0.1, but you can configure a different port and IP address if wish to send the messages to some other spam daemon running at a different location or on a different port.

MDSpamD Configuration

Host or IP
This is the host or IP address to which MDaemon will send messages to be scanned by MDSpamD. Use `127.0.0.1` if MDSpamD is running locally.

Port
This is the port on which the messages will be sent. The default MDSpamD port is 783.

Ping remote MDSpamD once every XX seconds (0=never)
If you are using a spam daemon that is running at a remote location, you can use this option to ping its location periodically. Use "0" if you do not wish to ping that location.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

These options are available when running MDSpamD locally

Show MDSpamD external process window
When MDSpamD is running locally, enable this option if you would like it to run in an external process window. This option will cause the output from MDSpamD to be piped to the external process window rather than to MDaemon's internal UI or logging system. Using this option could increase performance since MDSpamD's data will not have to be piped into and logged by MDaemon. However, no log file will be created and as such this feature cannot be used with the logging option below, nor will MDSpamD data appear in the *Security»MDSpamD* tab of MDaemon's main GUI.

Log all local MDSpamD activity (debug logging—performance drain)
Click this option if you wish to log all MDSpamD activity. This option is unavailable if you are using the *Show MDSpamD external process window* option above. Further, if using user credentials on the Windows Service 356 dialog rather than running MDaemon under the SYSTEM account, no MDSpamD activity will be logged.

When using this logging option, you may see decreased performance in your mail system, depending on your system and the level of activity. Generally you should only use this option for debugging purposes.

Maximum message processing threads (1-6)
This is the maximum number of threads that MDaemon will use for internal processing. You can set this value from 1 to 6.

Maximum TCP connections per thread (10-200)
This is the maximum number of TCP connections accepted by an MDSpamD thread before it branches into another thread. You can set this value from 10 to 200.

Listen on and accept connections only from 127.0.0.1
Click this option if do not you wish to allow your local MDSpamD to accept connections from any external source. Only connections from the same machine on which it is running will be allowed.

Listen for connections on this IP
If the previous option is disabled, you can use this option to bind or restrict connections to a specific IP address. Only connections to the designated IP address will be allowed. Use "<all>" if you do not wish to restrict MDSpamD to any particular IP address.

Allow connections from these IPs
These are the IP addresses from which MDSpamD will accept incoming connections. Connections from other IP addresses will be rejected. This is useful if you wish to allow connections from another server in order to share Spam Filter processing.

Optional command line options to pass to MDSpamD:

MDSpamD can accept many command line options, documented at:

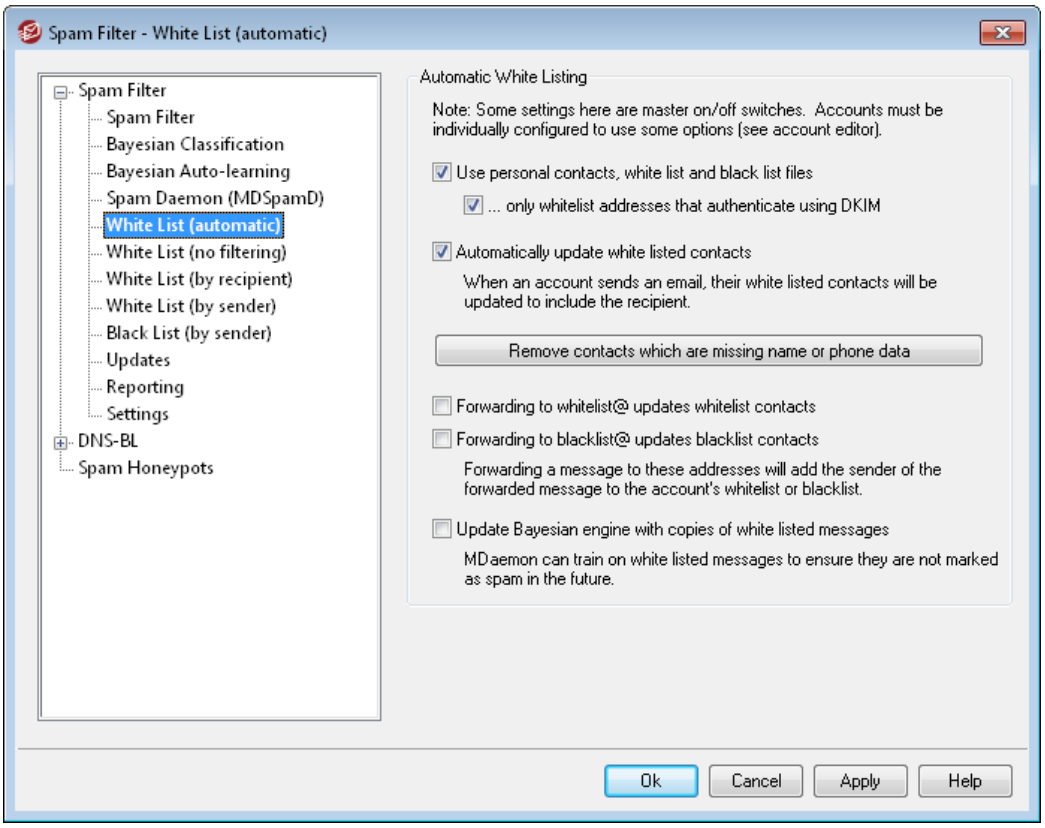
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

http://spamassassin.apache.org/

If you wish to use any of those options, construct a string containing the desired options and place it here.

Some of those options can be configured via the settings on this dialog and therefore do not need to be set up manually using command line options.

4.4.1.5 White List (automatic)


Spam Filter - White List (automatic)
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
Automatic White Listing
Note: Some settings here are master on/off switches. Accounts must be individually configured to use some options (see account editor).
Use personal contacts, white list and black list files
... only whitelist addresses that authenticate using DKIM
Automatically update white listed contacts
When an account sends an email, their white listed contacts will be updated to include the recipient.
Remove contacts which are missing name or phone data
Forwarding to whitelist@ updates whitelist contacts
Forwarding to blacklist@ updates blacklist contacts
Forwarding a message to these addresses will add the sender of the forwarded message to the account's whitelist or blacklist.
Update Bayesian engine with copies of white listed messages
MDaemon can train on white listed messages to ensure they are not marked as spam in the future.
Ok
Cancel
Apply
Help

Automatic White Listing

Use personal contacts, white list and black list files
Click this option to allow each user's personal contacts, white list and black list files to be used as Spam Filter white and black lists. For each incoming message, MDaemon will search the recipient account's contacts, white list, and black list for the sender of the message. If the sender is found then the message will be white or black listed automatically. If you do not wish to apply automatic white and black listing to every MDaemon user then you can disable it for individual users by clearing the *Spam Filter uses personal contacts, white list, and black list files* option on the White List 571 screen of the Account Editor.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Note: Keeping your contacts updated and synchronized with WorldClient, the Windows Address Book, and other MAPI mail clients that use the Windows Address Book can be easily done using WorldClient Instant Messenger 227.

...only whitelist addresses that authenticate using DKIM
When this option is enabled, MDaemon will not white list the message unless the sender was authenticated via DomainKeys Identified Mail 446 (DKIM). This option helps to avoid white listing messages with spoofed addresses.

Automatically update white listed contacts
When this option is enabled, MDaemon will automatically add any non-local email addresses to which you send mail to your personal white list folder. When used in conjunction with "*Use personal contacts, white list and black list files*" above, the number of Spam Filter false positives can be drastically reduced.

If you do not wish to apply automatic white list updating to every MDaemon user then you can disable it for individual users by clearing the "*Update white listed contacts with mail recipients*" check box on the White List 571 screen of the Account Editor.

This option is disabled for accounts using autoresponders.

Remove contacts which are missing name or phone data
Click this button if you wish to remove every contact that contains only an email address from every user's default Contacts folder. If a contact doesn't have at least a name or phone data it will be removed. The option is primarily to help those who have been using MDaemon's automatic white listing option prior to version 11 purge contacts that were added purely as a function of the white list feature. In previous versions of MDaemon the addresses were added to the main contacts instead of to a dedicated white list folder. This could result in users having many entries in their contacts that they would rather not have there.

Consider this option carefully before using it, because contacts containing only an email address could still be legitimate.

Forwarding to whitelist@ updates whitelist contacts
When this option is enabled, accounts using the "*Spam Filter uses personal contacts, white list, and black list files*" on the Account Editor's Settings screen can forward messages to `whitelist@<domain>` and have MDaemon add the sender of the original message to the account's white list. The white listed address is taken from the forwarded message's `From` header.

Messages forwarded to `whitelist@<domain>` must be forwarded as attachments of the type `message/rfc822`, and they must be received by MDaemon via SMTP from a session that is authenticated. Forwarded messages not meeting these requirements will not be processed.

You can change the address MDaemon uses by editing the following key in the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

CFILTER.INI file:

```
[SpamFilter]
WhiteListAddress=MyWhiteListAddress@
```

Note: the last character must be "@".

Forwarding to blacklist@ updates blacklist contacts
When this option is enabled, accounts using the "*Spam Filter uses personal contacts, white list, and black list files*" on the Account Editor's Settings screen can forward messages to blacklist@<domain> and have MDaemon add the sender of the original message to the account's black list. The black listed address is taken from the forwarded message's From header.

Messages forwarded to blacklist@<domain> must be forwarded as attachments of the type message/rfc822, and they must be received by MDaemon via SMTP from a session that is authenticated. Forwarded messages not meeting these requirements will not be processed.

Update Bayesian engine with copies of white listed messages
Check this box to cause qualified messages to be copied automatically into the Bayesian non-spam learning folder (designated on the Bayesian 405 screen). This helps to automate the process of providing the Bayesian engine with samples of non-spam messages. Regularly providing the Bayesian engine with new examples of non-spam to learn from will increase its reliability over time and help to reduce the number of false positives (i.e. messages that are erroneously classified as spam).

To qualify for this feature, an incoming message must be addressed to a local user and the sender must be someone in his address book file. If the message is outgoing, then it must be the recipient who is in the address book. If you do not want any outgoing messages to qualify, then use Notepad to edit the following setting in the MDaemon.ini file:

```
[SpamFilter]
UpdateHamFolderOutbound=No (default = Yes)
```

When a message qualifies, it is copied into the Bayesian non-spam learning folder even if Bayesian scheduled learning is disabled on the Bayesian screen. Thus, when scheduled learning is later enabled, or when learning is manually activated, a set of non-spam messages will be ready for analysis. Not every message that qualifies, however, is copied into the learning folder. When the feature is activated, MDaemon will copy qualified messages until a designated number is reached. Subsequently it will copy single messages at designated intervals. By default, the first 200 qualifying messages will be copied and then every tenth qualifying message after that. The initial number copied is equal to the number designated in the option, "*Non-spam samples needed before Bayesian scoring is possible*" located on the Bayesian Auto-learning 409 screen. Changing that setting will also change this value. If you wish to change the interval by which subsequent messages are copied, you can do so by editing the following setting in the MDaemon.ini file:

```
[SpamFilter]
HamSkipCount=10 (default = 10)
```

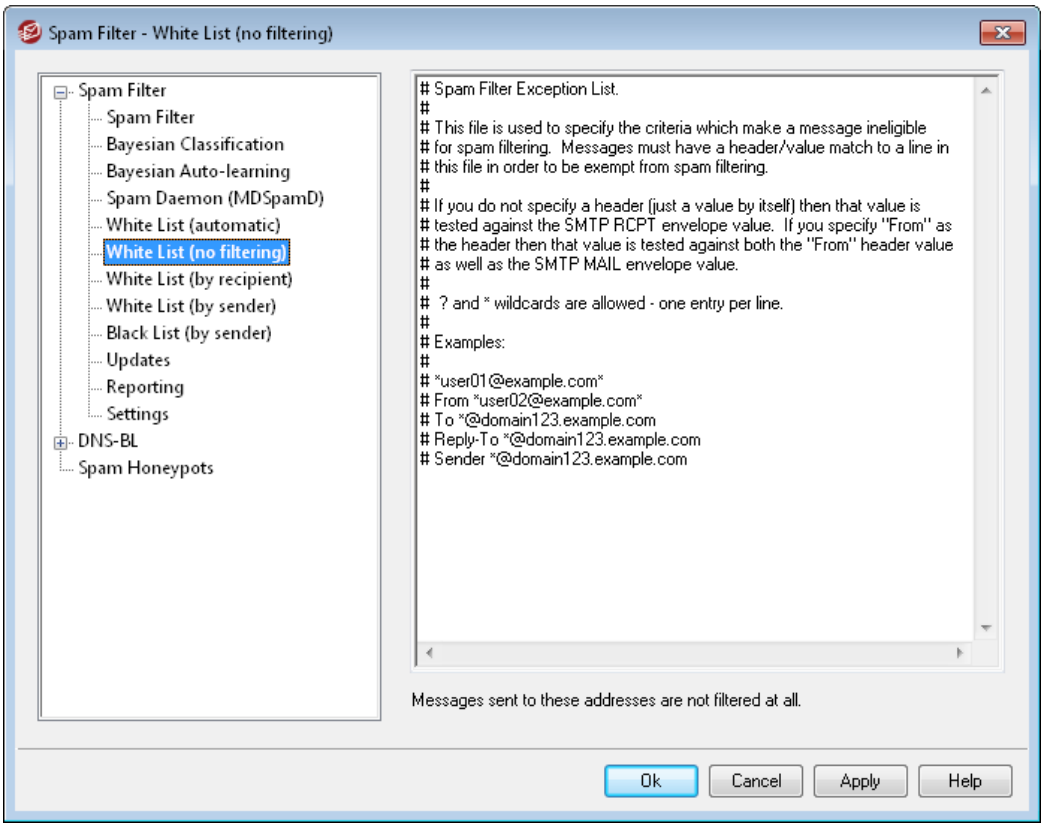
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Finally, once a designated total number of messages has been copied, the entire process will be begin again — 200 will be copied and then every tenth (or an alternate value if you have changed these settings). By default, the process will be restarted after 500 qualifying messages have been copied. You can change this value by editing the following setting in the `MDaemon.ini` file:

```
[SpamFilter]
HamMaxCount=500 (default = 500)
```

This option is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. All Bayesian learning functions are determined by the other server's settings and are performed on the other server. See Spam Daemon 411 for more information.

4.4.1.6 White List (no filtering)

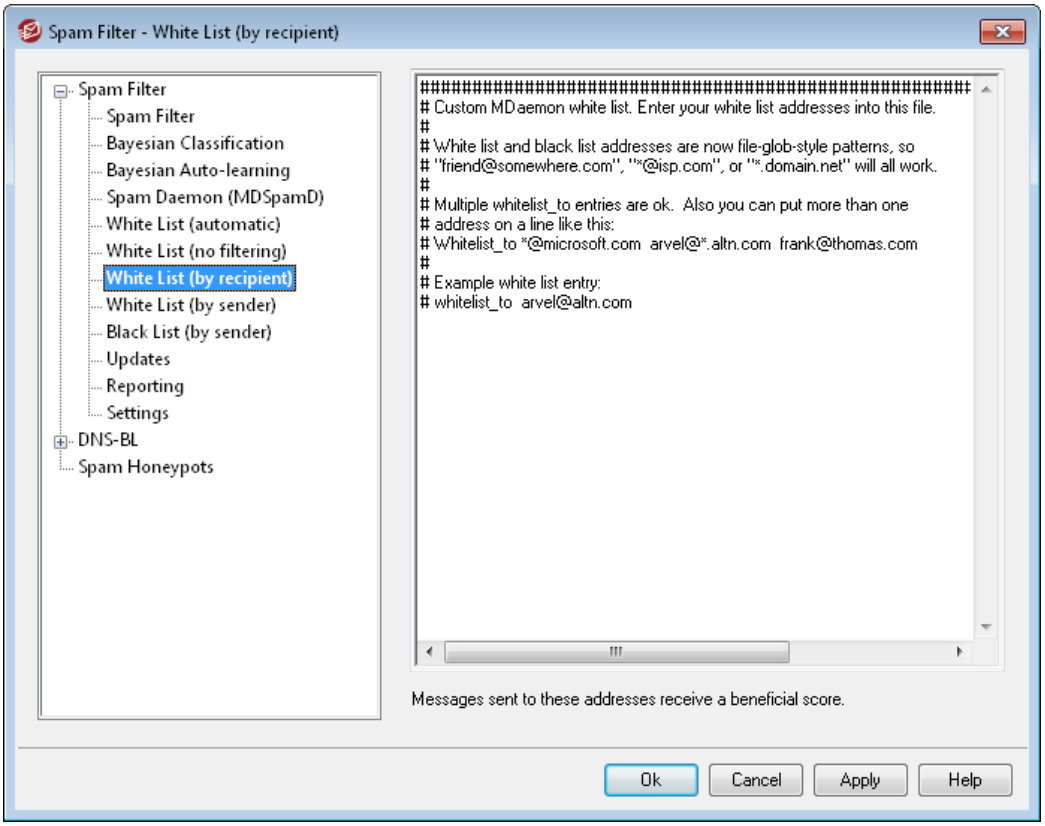

Spam Filter - White List (no filtering)
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
Spam Filter Exception List.
#
This file is used to specify the criteria which make a message ineligible
for spam filtering. Messages must have a header/value match to a line in
this file in order to be exempt from spam filtering.
#
If you do not specify a header (just a value by itself) then that value is
tested against the SMTP RCPT envelope value. If you specify "From" as
the header then that value is tested against both the "From" header value
as well as the SMTP MAIL envelope value.
#
? and * wildcards are allowed - one entry per line.
#
Examples:
#
user01@example.com
From *user02@example.com*
To *@domain123.example.com
Reply-To *@domain123.example.com
Sender *@domain123.example.com
Messages sent to these addresses are not filtered at all.
Ok
Cancel
Apply
Help

Messages sent to these addresses are not filtered at all
Use this screen to designate recipient addresses that you wish to be exempt from spam filtering. Messages destined for these addresses will not be processed through the spam filter.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 411 for more information.

4.4.1.7 White List (by recipient)

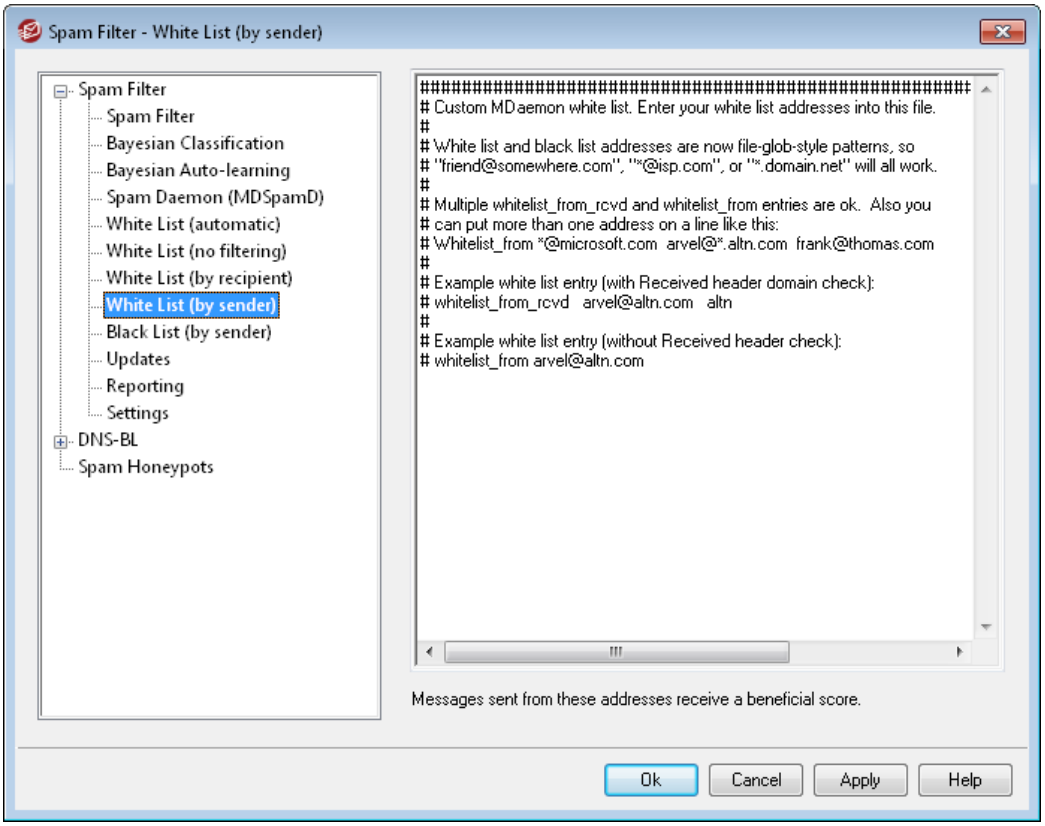

Spam Filter - White List (by recipient)
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
Custom MDaemon white list. Enter your white list addresses into this file.
White list and black list addresses are now file-glob-style patterns, so
"friend@somewhere.com", "*@isp.com", or "*.domain.net" will all work.
Multiple whitelist_to entries are ok. Also you can put more than one
address on a line like this:
Whitelist_to *@microsoft.com arvel@*.altn.com frank@thomas.com
Example white list entry:
whitelist_to arvel@altn.com
Messages sent to these addresses receive a beneficial score.
Ok
Cancel
Apply
Help

Messages sent to these addresses receive a beneficial score
This list is similar to *White List (no filtering)* 416, except that rather than exempting messages for the recipient from Spam Filter processing, they will be processed but have their Spam Filter score 402 reduced by the amount specified on the Spam Filter Settings 422 screen. Therefore including an address on this white list does not automatically guarantee that a message to that address will not be considered spam. For example, if you have the spam score threshold set to 5.0 and the white list value set to 100, and then a particularly excessive spam message arrives that gets a spam score of 105.0 or higher before the white list value is subtracted, then the final spam score of the message will be at least 5.0, thus denoting it as spam. This is highly unlikely, however, because spam rarely has a value that high unless it contains some other exceptionally high-scoring element, such as a blacklisted address.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 411 for more information.

4.4.1.8 White List (by sender)

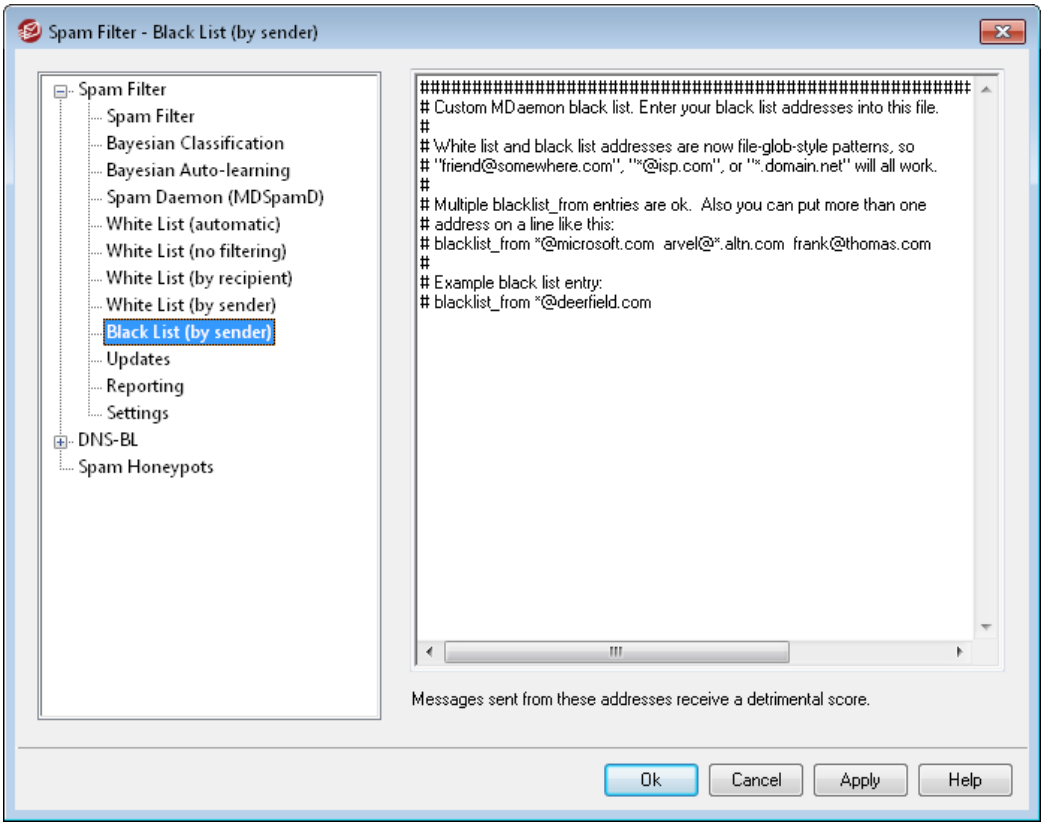

Spam Filter - White List (by sender)
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
Custom MDaemon white list. Enter your white list addresses into this file.
White list and black list addresses are now file-glob-style patterns, so
"friend@somewhere.com", "*@isp.com", or "*.domain.net" will all work.
Multiple whitelist_from_rcvd and whitelist_from entries are ok. Also you
can put more than one address on a line like this:
Whitelist_from *@microsoft.com arvel@*.altn.com frank@thomas.com
Example white list entry (with Received header domain check):
whitelist_from_rcvd arvel@altn.com altn
Example white list entry (without Received header check):
whitelist_from arvel@altn.com
Messages sent from these addresses receive a beneficial score.
Ok
Cancel
Apply
Help

Messages sent from these addresses receive a beneficial score
This white list is similar to *White List (by recipient)* 417, except that spam score reduction is based on who the message is *from* rather than based on the recipient. Messages from these senders will have their Spam Filter score 402 reduced by the amount specified on the Spam Filter Settings 422 screen. Therefore including an address on this white list does not automatically guarantee that a message to that address will not be considered spam. For example, if you have the spam score threshold set to 5.0 and the white list value set to 100, and then a particularly excessive spam message arrives that gets a spam score of 105.0 or higher before the white list value is subtracted, then the final spam score of the message will be at least 5.0, thus denoting it as spam. This is highly unlikely, however, because spam rarely has a value that high unless it contains some other exceptionally high-scoring element, such as a blacklisted address.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 411 for more information.

4.4.1.9 Black List (by sender)


Spam Filter - Black List (by sender)
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
Custom MDaemon black list. Enter your black list addresses into this file.
White list and black list addresses are now file-glob-style patterns, so
"friend@somewhere.com", "*@isp.com", or "*.domain.net" will all work.
Multiple blacklist_from entries are ok. Also you can put more than one
address on a line like this:
blacklist_from *@microsoft.com arvel@*.altn.com frank@thomas.com
Example black list entry:
blacklist_from *@deerfield.com
Messages sent from these addresses receive a detrimental score.
Ok
Cancel
Apply
Help

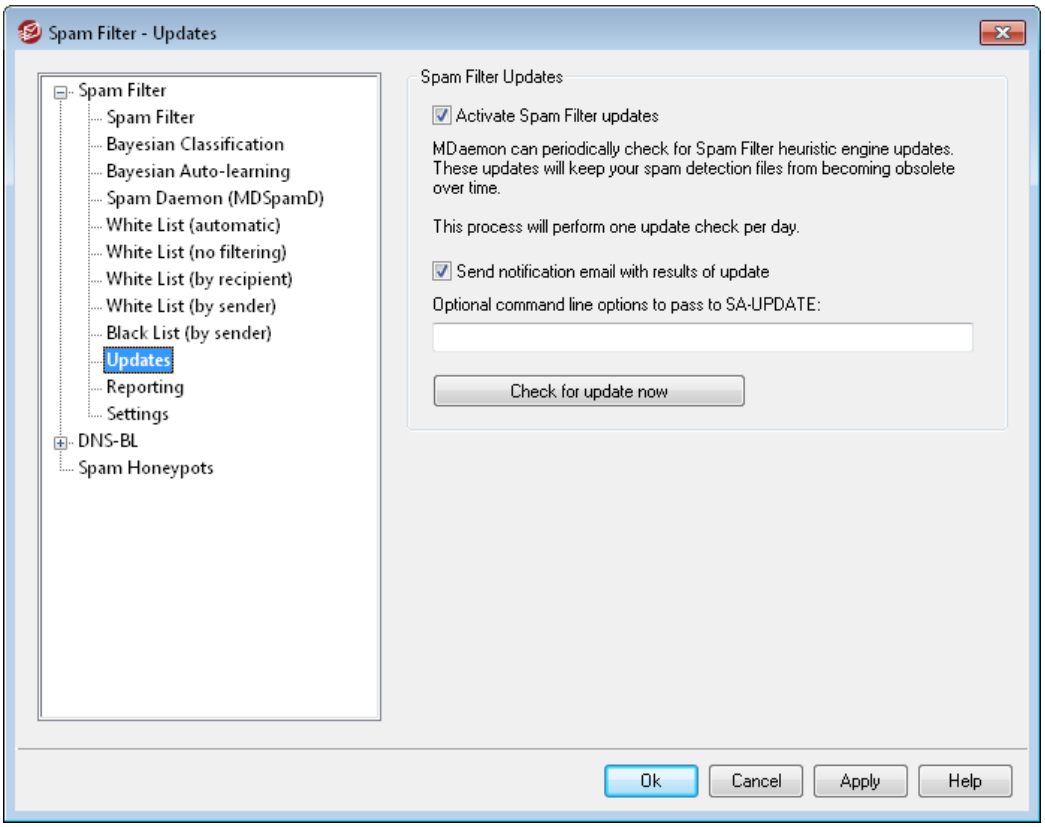
Messages sent from these addresses receive a detrimental score
Messages from addresses on this black list will have their Spam Filter score 402 increased by the amount specified on the Spam Filter Settings 422 screen, typically causing them to be marked as spam. However, including an address on this list does not automatically guarantee that a message from that address will always be considered spam. For example, if a message comes from a black listed sender but is addressed to a white listed recipient, then the score modifiers may offset each other and cause the message to have a final score that is below the spam score threshold. This could also happen if you have the black list score modifier set particularly low.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD)

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 411 for more information.

4.4.1.10 Updates



Spam Filter Updates

Activate Spam Filter updates
Click this check box if you want the Spam Filter be updated automatically. Once per day MDaemon will to see if there are any updates available for the Spam Filter heuristics engine, and if so it will download and install them automatically.

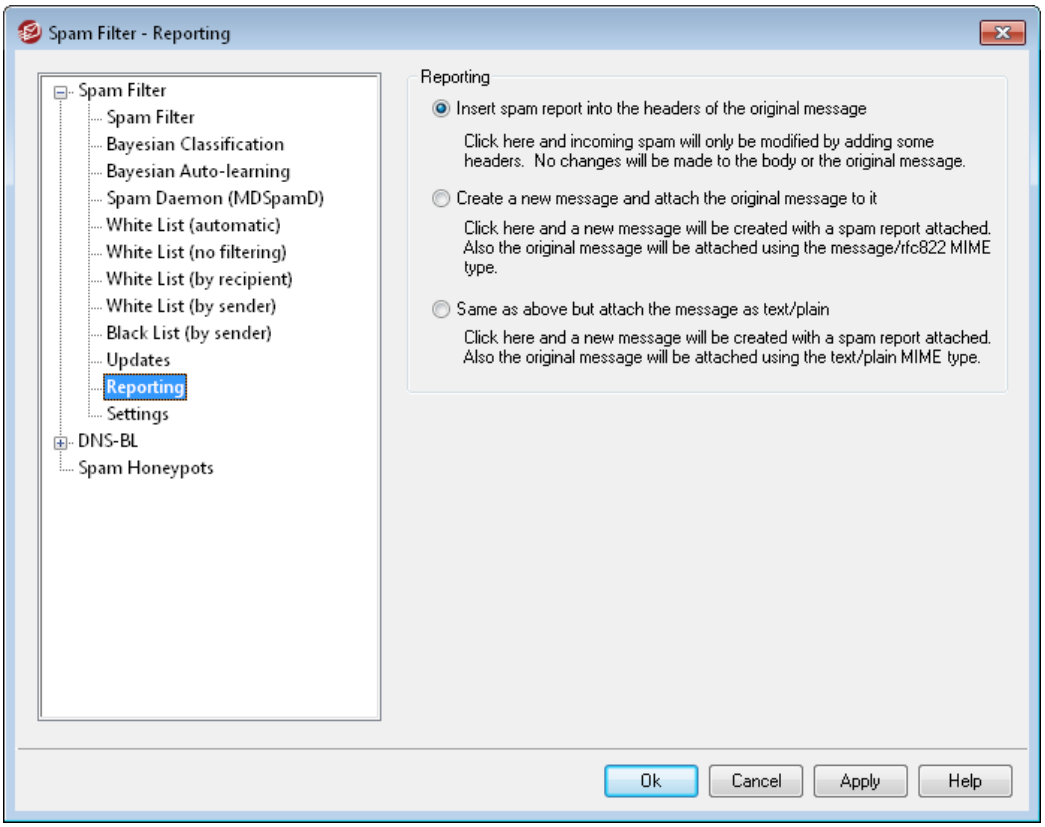
Send notification email with results of update
Use this option if you wish to send an email to the administrators whenever the Spam Filter is updated, containing the results of the update. This option is the same as the "*Send Spam Filter update notification to Administrators*" option located at: Content Filter » Notifications.

Optional command line options to pass to SA-UPDATE
Use this advanced option if you wish to pass any command line options to SA-UPDATE.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Check for update now
Click this button to check immediately for a Spam Filter rules update.

4.4.1.11 Reporting


Spam Filter - Reporting
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
Reporting
Insert spam report into the headers of the original message
Click here and incoming spam will only be modified by adding some headers. No changes will be made to the body or the original message.
Create a new message and attach the original message to it
Click here and a new message will be created with a spam report attached. Also the original message will be attached using the message/rfc822 MIME type.
Same as above but attach the message as text/plain
Click here and a new message will be created with a spam report attached. Also the original message will be attached using the text/plain MIME type.
Ok
Cancel
Apply
Help

The Spam Filter Reporting options are unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. Spam Filter Reporting will be controlled by the other server's settings. See the Spam Daemon 411 screen for more information.

Reporting

Insert spam report into the headers of the original message
This is the default reporting option. Use this option if you want the Spam Filter to insert a spam report into each spam message's headers. The following is an example of a simple spam report:

```
X-Spam-Report: ---- Start Spam Filter results
  5.30 points, 5 required;
  * -5.7 -- Message-Id indicates the message was sent from MS Exchange
  *  2.0 -- Subject contains lots of white space
  * -3.3 -- Has a In-Reply-To header
```

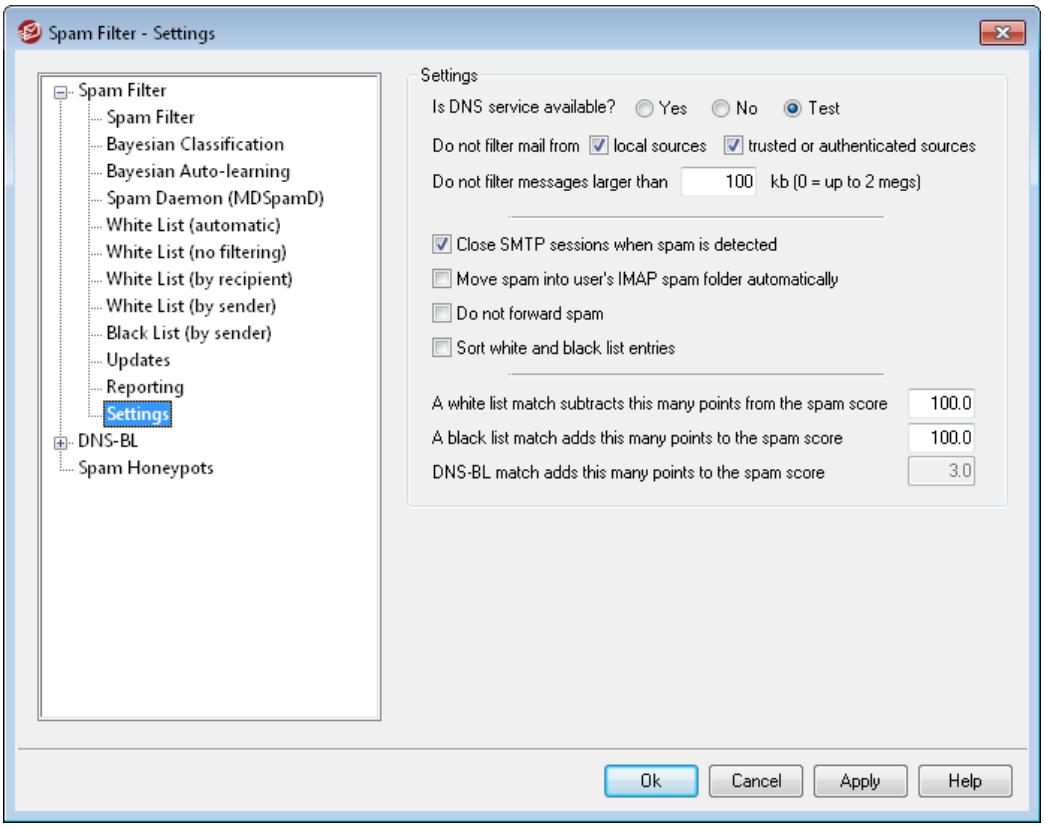
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

```
  *  3.0 -- Message has been marked by MDaemon's DNS-BL
  *  2.9 -- BODY: Impotence cure
  *  2.2 -- BODY: Talks about exercise with an exclamation!
  *  0.5 -- BODY: Message is 80% to 90% HTML
  *  0.1 -- BODY: HTML included in message
  *  1.6 -- BODY: HTML message is a saved web page
  *  2.0 -- Date: is 96 hours or more before Received: date
---- End of Spam Filter results
```

Create a new message and attach the original message to it
Choose this reporting option if you want spam to cause a new email message to be created containing the spam report. The original spam message will be included with it as a file attachment.

Same as above but attach the message as text/plain
Like the previous reporting option, this option will generate the spam report as a new message that includes the original spam message as a file attachment. The difference is that the original message will be attached using the text/plain MIME type. Because spam sometimes contains HTML code that is unique for each message and can potentially reveal to the spammer which email and IP address opened it, this method can prevent that from happening by converting the HTML code to plain text.

4.4.1.12 Settings


Spam Filter - Settings
Spam Filter
Spam Filter
Bayesian Classification
Bayesian Auto-learning
Spam Daemon (MDSpamD)
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Updates
Reporting
Settings
DNS-BL
Spam Honeypots
Settings
Is DNS service available? Yes No Test
Do not filter mail from local sources trusted or authenticated sources
Do not filter messages larger than 100 kb (0 = up to 2 megs)
Close SMTP sessions when spam is detected
Move spam into user's IMAP spam folder automatically
Do not forward spam
Sort white and black list entries
A white list match subtracts this many points from the spam score 100.0
A black list match adds this many points to the spam score 100.0
DNS-BL match adds this many points to the spam score 3.0
Ok
Cancel
Apply
Help

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Settings

Is DNS service available?
These options allow you to choose whether or not DNS is available to the Spam Filter when processing messages. You may choose one of the following options:

Yes - DNS is available. SURBL/RBL and other rules that require DNS connectivity will therefore be utilized.

No - DNS is not available. Spam filtering rules that require DNS will not be utilized.

Test - DNS availability will be tested and if present it will be used. This is the default setting.

Don't filter mail from...

local sources
Click this check box if you want messages from local users and domains to be exempt from filtering.

trusted or authenticated sources
Enable this option if you want messages sent from trusted domains or authenticated senders to be exempt from spam filtering.

Don't filter messages larger than [XX] kb (0=up to 2MB)
It is typical for spam messages to be fairly small since the usual goal of the spammers is to deliver as many messages as possible in the shortest amount of time. If you want messages over a certain size to be exempt from spam filtering then specify the size (in KB) here. Use "0" if you want only very large messages to be exempt from spam filtering—only messages over 2MB will not be filtered.

Close SMTP sessions when spam is detected
This option is enabled by default and will close an SMTP session if an inline scan detects a spam message.

Move spam into user's IMAP spam folder automatically
Click this option and MDaemon will automatically place each message that the Spam Filter determines to be spam into each user's "Spam" IMAP folder (if such a folder exists). It will also automatically create the folder for each new user account that is added.

When you click this option you will also be asked whether or not you would like MDaemon to create this folder for each of your already existing user accounts. If you choose "Yes" then a folder will be created for all users. If you choose "No" then a folder will only be created when each new user is added. Any folders that already exist for some or all of your users will not be altered or affected in any way.

Don't forward spam
Click this check box if you do not wish to allow spam messages to be forwarded.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Sort white and black list entries
Use this option if you wish to keep the Spam Filter white and black list entries in sorted sequence. **Note:** if you have added your own comments to the file (lines starting with #), enabling this option will sort these lines to the top of the file. This feature is disabled by default. If you enable the option, the sort will take place upon the next change to the white or black list file.

The remaining options on this screen are unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. See the Spam Daemon 411 screen for more information.

A white list match subtracts this many points from the spam score
Placing an address on the Spam Filter's White List (by recipient) 417 or White List (by sender) 418 screens does not automatically guarantee that a message to or from that address will not be considered spam. Instead, those white listed addresses will simply have the amount specified in this control subtracted from their spam scores. For example, if you have the spam score threshold set to 5.0 and this value set to 100, and then a particularly excessive spam message arrives that gets a spam score of 105.0 or higher before the white list value is subtracted, then the final spam score of the message will be at least 5.0 — thus denoting it as spam. This would rarely happen, however, because spam rarely has a value that high unless it contains some other exceptionally high-scoring element, such as a blacklisted address. Of course, if you set the white list subtraction value to a much lower amount then it would occur much more frequently.

If you wish to cause messages addressed to certain recipients to bypass the Spam Filter completely rather than simply adjust their scores, include those recipient addresses on the White List (no filtering) 416 screen. You can also exclude messages from Spam Filter scoring based on the sender by using the options on the White List (automatic) 413 screen.

A black list match adds this many points to the spam score
This value is added to the spam score of messages from addresses found on the Black List (by sender) 419 screen. As with the white list option above, including an address on the Spam Filter's black list doesn't guarantee that a message from that address will be considered spam. Instead, the value specified in this option will be added to the message's spam score, which will then be used to determine whether or not the message is spam.

DNS-BL match adds this many points to the spam score
If you are using DNS Black Lists 425 then you can use this option to specify a value that will be added to a message's spam score when a DNS-BL match is found. Sometimes the Spam Filter's heuristic examination of a message may not score it high enough to be considered spam, but a DNS-BL lookup may show that it probably

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

is spam. Adding this value to the spam score of these messages can help to reduce the number of spam messages that manage to slip through undetected by the Spam Filter.

4.4.2 DNS Black Lists (DNS-BL)

DNS Black Lists (DNS-BL) can be used to help prevent spam email from reaching your users. This security feature allows you to specify several DNS blacklisting services (which maintain lists of servers known to relay spam) that will be checked each time someone tries to send a message to your server. If the connecting IP has been blacklisted by any one of these services, the message(s) will be refused or flagged according to the settings on the Settings 428 screen.

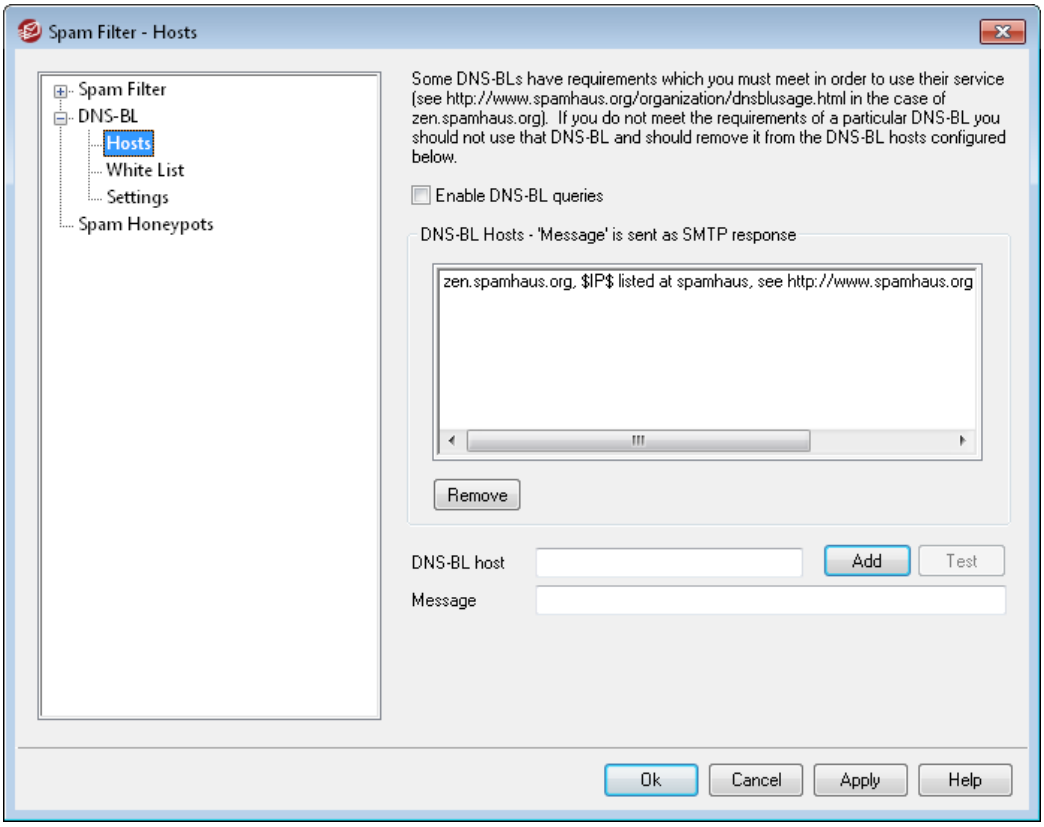
DNS Black Lists includes a White List for designating IP addresses that you wish to make exempt from DNS-BL queries. Before activating DNS-BL, you should make sure that your local IP address range is on the White List to prevent lookups on those addresses. "127.0.0.1" is exempt and therefore doesn't need to be added to the list.

See:

DNS-BL Hosts 426
DNS-BL Settings 428
DNS-BL White List 427

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.4.2.1 Hosts


Spam Filter - Hosts
Spam Filter
DNS-BL
Hosts
White List
Settings
Spam Honeypots
Some DNS-BLs have requirements which you must meet in order to use their service (see http://www.spamhaus.org/organization/dnsblusage.html in the case of zen.spamhaus.org). If you do not meet the requirements of a particular DNS-BL you should not use that DNS-BL and should remove it from the DNS-BL hosts configured below.
Enable DNS-BL queries
DNS-BL Hosts - 'Message' is sent as SMTP response
zen.spamhaus.org, IP listed at spamhaus, see http://www.spamhaus.org
Remove
DNS-BL host
Add
Test
Message
Ok
Cancel
Apply
Help

DNS-BL Hosts

Enable DNS-BL queries
Activate this option if you wish to check incoming mail against DNS Black Lists. MDaemon will query each listed host when performing a DNS-BL lookup on the sending IP address. If a host replies to the query with a positive result, MDaemon can flag the message or refuse to accept it, depending on which options you have enabled on the DNS-BL Settings 428 screen.

Remove
Select an entry from the DNS-BL service list and click this button to remove it from the list.

DNS-BL host
If you wish to add a new host to be queried for blacklisted IP addresses, enter it here.

Test
Enter a host into the *DNS-BL host* option and click this button to test it by looking up 127.0.0.2.

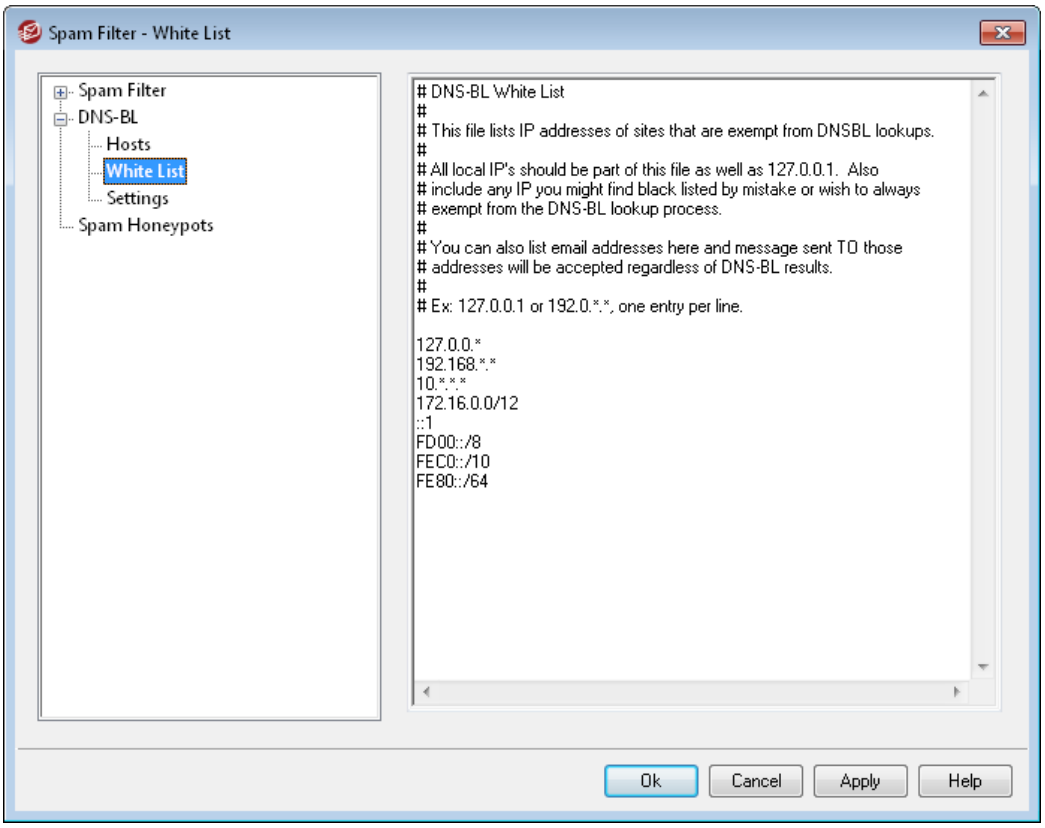
Message
This is the message that can be sent during the SMTP session when an IP address

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

has been blacklisted by the corresponding DNS-BL host listed above. This message corresponds to the *...and respond with 'Message' rather than 'user unknown'* option located on the DNS-BL Settings 428 screen.

Add
After entering a host and return message, click this button to add it to the DNS-BL hosts list.

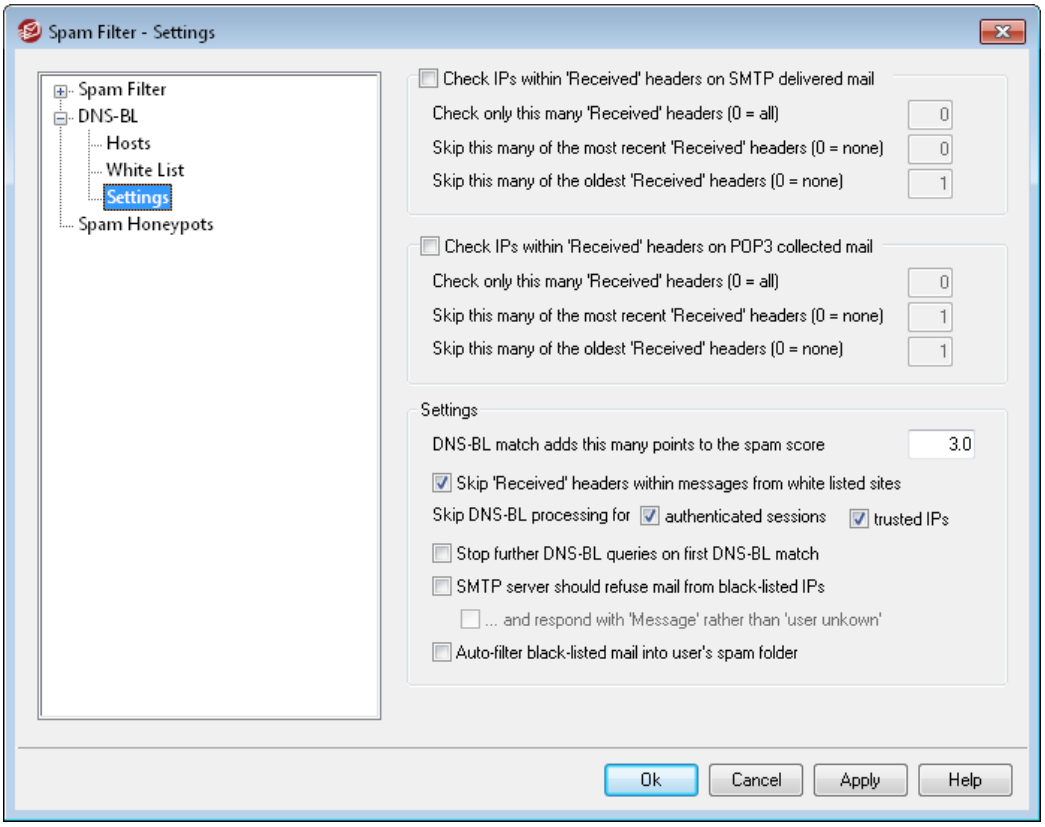
4.4.2.2 White List



Use this screen to designate IP addresses that will be exempt from DNS Black List queries. You should always include your local IP address range to prevent DNS-BL from looking up messages originating from local users and domains (i.e. `127.0.0.*`, `192.168.*.*`, and so on). Place one address on each line. Wildcards are permitted.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.4.2.3 Settings


Spam Filter - Settings
Spam Filter
DNS-BL
Hosts
White List
Settings
Spam Honeypots
Check IPs within 'Received' headers on SMTP delivered mail
Check only this many 'Received' headers (0 = all)
Skip this many of the most recent 'Received' headers (0 = none)
Skip this many of the oldest 'Received' headers (0 = none)
Check IPs within 'Received' headers on POP3 collected mail
Check only this many 'Received' headers (0 = all)
Skip this many of the most recent 'Received' headers (0 = none)
Skip this many of the oldest 'Received' headers (0 = none)
Settings
DNS-BL match adds this many points to the spam score
Skip 'Received' headers within messages from white listed sites
Skip DNS-BL processing for authenticated sessions trusted IPs
Stop further DNS-BL queries on first DNS-BL match
SMTP server should refuse mail from black-listed IPs
... and respond with 'Message' rather than 'user unkown'
Auto-filter black-listed mail into user's spam folder
Ok
Cancel
Apply
Help

Check IPs within 'Received' headers on SMTP delivered mail
Click this switch if you want DNS Black Lists to check the IP address stamped in the "Received" headers of messages received via SMTP.

Check only this many 'Received' headers (0 = all)
Specify the number of "Received" headers that you want DNS-BL to check, starting with the most recent. A value of "0" means that all "Received" headers will be checked.

Skip this many of the most recent 'Received' headers (0 =none)
Use this option if you want DNS-BL to skip over one or more of the most recent Received headers when checking SMTP messages.

Skip this many of the oldest 'Received' headers (0 =none)
Use this option if you want DNS-BL to skip over one or more of oldest Received headers when checking SMTP messages.

Check IPs within 'Received' headers on POP3 collected mail
When this switch is enabled DNS-BL will check the IP address stamped in the "Received" headers of messages collected via DomainPOP and MultiPOP.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Check only this many 'Received' headers (0 = all)
Specify the number of 'Received' headers that you want DNS-BL to check, starting with the most recent. A value of "0" means that all 'Received' headers will be checked.

Skip this many of the most recent 'Received' headers (0 =none)
Use this option if you want DNS-BL to skip over one or more of the most recent Received headers when checking DomainPOP and MultiPOP messages. Since it is often necessary to skip the most recent Received header on POP3 collected mail such as DomainPOP, this option has a default setting of "1".

Skip this many of the oldest 'Received' headers (0 =none)
Use this option if you want DNS-BL to skip over one or more of the oldest Received headers when checking DomainPOP and MultiPOP messages.

Settings

DNS-BL match adds this many points to the spam score
This is the number of points that will be added to a message's spam score 402 when there is a DNS Black List match. By default this adds 3.0 points.

Skip 'Received' headers within messages from white listed sites
When this option is enabled, DNS-BL will not check the "Received" headers within messages coming from IP addresses that you have listed on the DNS-BL White List 427.

Skip DNS-BL processing for:

authenticated sessions
Click this checkbox if you want those sessions that were authenticated using the AUTH command to be exempt from DNS-BL queries.

trusted IPs
Click this checkbox if you want addresses that are listed on the Trusted Hosts 438 screen to be exempt from DNS-BL queries.

Stop further DNS-BL queries on first DNS-BL match
Oftentimes there are multiple hosts contained in the headers of each message that DNS-BL processes, and multiple DNS-BL services that are queried. By default, DNS-BL will continue to query these services for all hosts in the message regardless of the number of matches found. Click this option if you want DNS-BL to stop querying the services for any given message as soon as a match is found.

SMTP server should refuse mail from black-listed IPs
By default this box is unchecked, meaning that messages from blacklisted IP addresses will not be refused during the SMTP session, but will have an X-MDDNSBL-Result header inserted. You can then use the Content Filter to search for messages with this header and do with them as you please. You can also use the "*Auto-filter black-listed mail into user's spam folder*" option below to filter messages automatically into each user's spam folder. Check this box if you wish MDaemon to refuse messages from blacklisted IP addresses rather than flag them.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Because some IP addresses can be blacklisted by mistake, you should exercise caution before choosing to refuse messages rather than simply flagging them. It is also worth noting that in addition to flagging a message, you can adjust its spam score based on the DNS-BL results via the *DNS-BL match adds this many points to the spam score* option located on the Spam Filter 402.

...and respond with 'Message' rather than 'user unknown'
Click this option if you want the specific Message you have assigned to the DNS-BL Host 426 to be passed during the SMTP session whenever an IP address is found to be blacklisted. Otherwise, a "user unknown" message will be passed instead. This option is only available if you have elected to use the "*SMTP server should refuse mail from black-listed IPs*" option above.

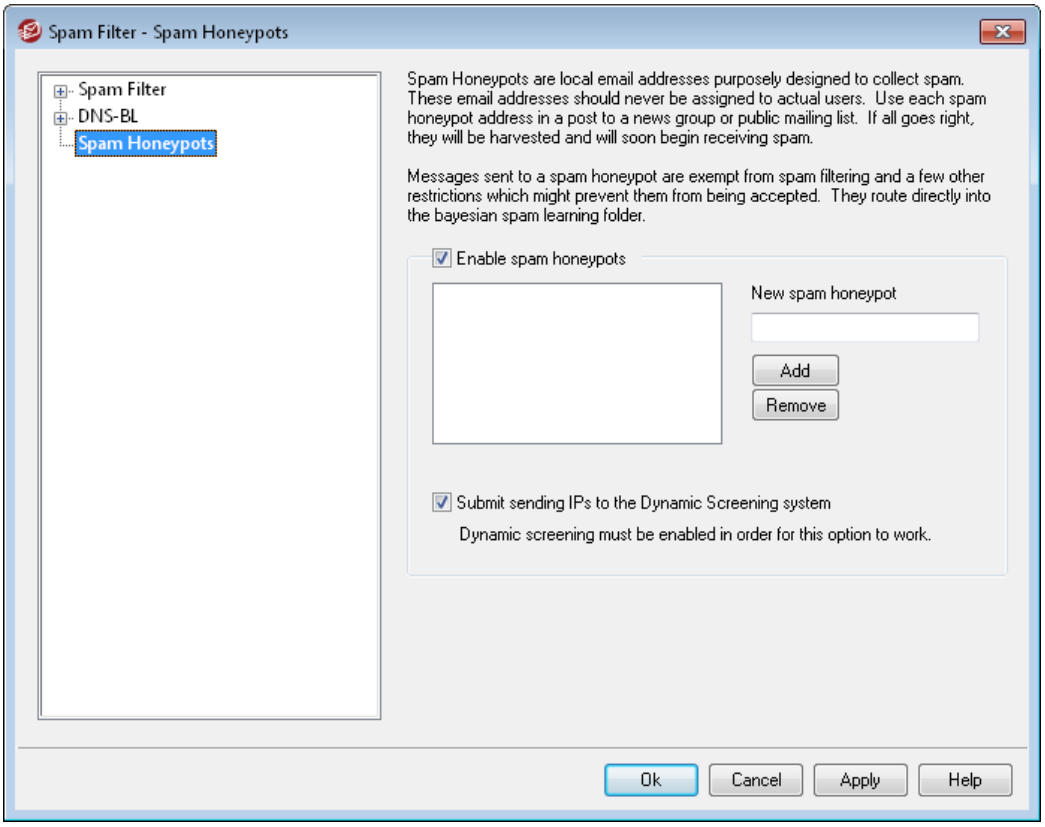
Auto-filter black-listed mail into user's spam folder
Click this option and a "Junk E-mail" IMAP folder will be created for all future user accounts that you add to MDaemon. MDaemon will also create a mail filter for each of those users, which will search for the X-MDDNSBL-Result header and then place messages containing that header into the user's spam folder. When you click this option you will also be asked whether or not you would like MDaemon to create this folder and filter for each of your already existing user accounts. See *Auto-generating a Spam Folder and Filter for Each Account* below.

Auto-generating a Spam Folder and Filter for Each Account

MDaemon can automatically create a "Junk E-mail" IMAP mail folder for each account and generate a mail filter that will move messages into that folder whenever if finds the `X-MDDNSBL-Result` header. Whenever you click the *Auto-filter black-listed mail into user's spam folder* option, you will be presented with the option to create the folder and accompanying filter for all accounts. Simply choose “yes” on the dialog to create the folders and filters. Although not foolproof, this is an easy and generally reliable way to help your users quickly identify spam email messages—it can effectively prevent spam email from being mixed in with all of their legitimate email. They will only occasionally need to review the contents of their spam folder just to make sure that an important message doesn't accidentally get put there (which may sometimes occur). When creating the folders and filters for your accounts, if MDaemon finds that an account already has a filter that checks for the existence of the `X-MDDNSBL-Result` header then no action will be taken and no filter will be created for that account. If you want the name of the IMAP folder to be something other than "Junk E-mail", you can change the default setting by editing the *Default spam folder name* option located on the System 347 screen under `Setup » Preferences`.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.4.3 Spam Honeypots


Spam Filter - Spam Honeypots
Spam Filter
DNS-BL
Spam Honeypots
Spam Honeypots are local email addresses purposely designed to collect spam. These email addresses should never be assigned to actual users. Use each spam honeypot address in a post to a news group or public mailing list. If all goes right, they will be harvested and will soon begin receiving spam.
Messages sent to a spam honeypot are exempt from spam filtering and a few other restrictions which might prevent them from being accepted. They route directly into the bayesian spam learning folder.
Enable spam honeypots
New spam honeypot
Add
Remove
Submit sending IPs to the Dynamic Screening system
Dynamic screening must be enabled in order for this option to work.
Ok
Cancel
Apply
Help

Spam Honeypots (located at Security » Spam Filter » Spam Honeypots) is for designating local email addresses purposely designed to collect spam. These spam honeypots are not valid MDaemon accounts or address aliases and should never be used for sending or receiving legitimate email. But, by posting a honeypot address to a news group, public mailing list, or other source from which spammers often farm addresses, you should begin to see incoming messages addressed to the spam honeypots — you could also pull addresses from other spam that you have received addressed to other invalid local addresses. Because honeypots will never receive legitimate email, all incoming messages addressed to them will always be routed directly to your Bayesian spam trap folder for processing. Further, the IP addresses of the sending servers can optionally be added to the Dynamic Screening 482 system, banning future connections from those addresses for a designated period of time. All of this helps increase the probability of identifying and blocking spam in the future.

Spam Honeypots

This list contains all addresses that you have designated as Spam Honeypots.

Enable spam honeypots
This option is enabled by default. Uncheck this box if you wish to disable the spam honeypots feature.

New spam honeypot
To add a spam honeypot, enter the address here and click *Add*.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

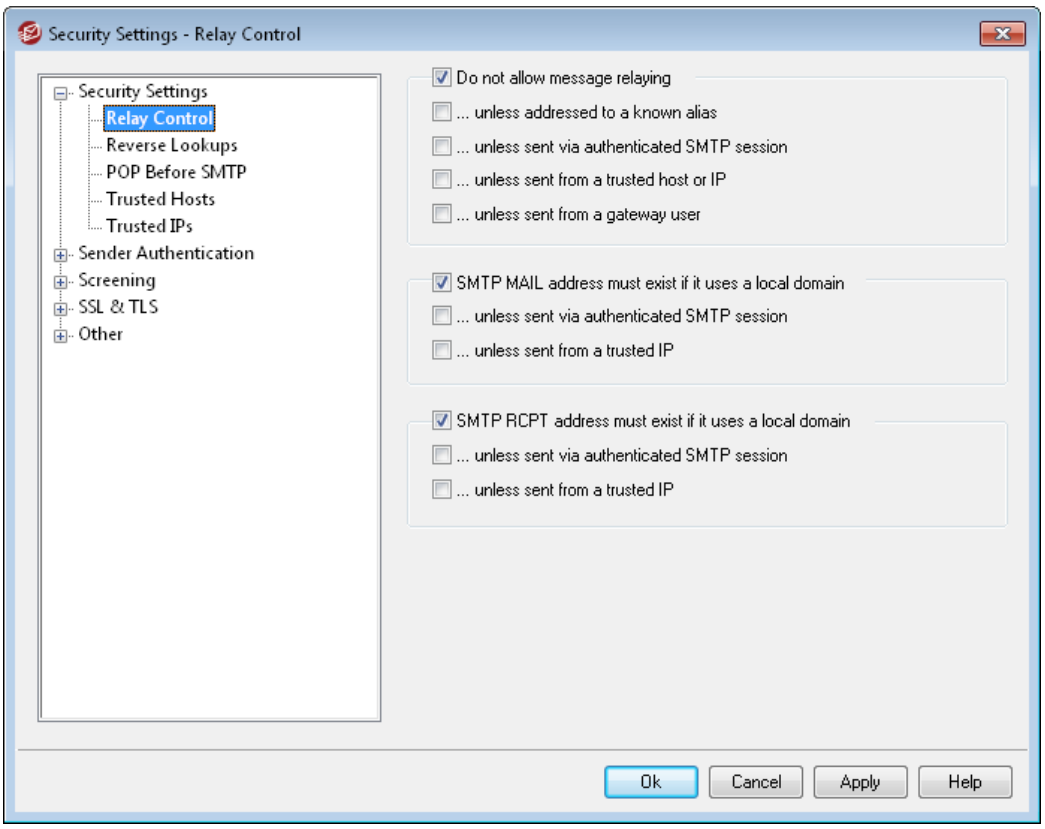
Remove
To remove a spam honeypot, select the desired address and then click Remove.

Submit sending IPs to the Dynamic Screening system
Check this box if you wish to submit to the Dynamic Screening 482 system all IP addresses from which a Spam Honeypots message arrives. The Dynamic Screen (located at Security » Security Settings » Screening » Dynamic Screen) must be enabled on your server before this feature will be available.

4.5 Security Settings

4.5.1 Security Settings

4.5.1.1 Relay Control


Security Settings - Relay Control
Security Settings
Relay Control
Reverse Lookups
POP Before SMTP
Trusted Hosts
Trusted IPs
Sender Authentication
Screening
SSL & TLS
Other
Do not allow message relaying
... unless addressed to a known alias
... unless sent via authenticated SMTP session
... unless sent from a trusted host or IP
... unless sent from a gateway user
SMTP MAIL address must exist if it uses a local domain
... unless sent via authenticated SMTP session
... unless sent from a trusted IP
SMTP RCPT address must exist if it uses a local domain
... unless sent via authenticated SMTP session
... unless sent from a trusted IP
Ok
Cancel
Apply
Help

Use Relay Control at Security » Security Settings » Relay Control to define how your server reacts to mail relaying. When a message arrives at your mail server that is neither from nor to a local address, your server is being asked to relay (i.e. deliver) the message on behalf of another server. If you do not want your server to relay mail for unknown users, you can use the settings provided here to control that.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Relaying email indiscriminately for other servers could result in your domain being blacklisted by one or more DNS-BL services 425. Open relaying is greatly discouraged because spammers exploit open servers to hide their tracks.

Mail Relaying

Do not allow message relaying
When this option is enabled, MDaemon will refuse to accept messages for delivery that are both `FROM` and `TO` a non-local user.

...unless addressed to a known alias
Click this checkbox if you want MDaemon to relay mail for Aliases 613 regardless of your Relay settings.

...unless sent via authenticated SMTP session
When this checkbox is enabled, MDaemon will always relay mail when it is sent via an authenticated SMTP session.

...unless sent from a trusted host or IP
Enable this option is you wish to allow relaying when the mail is coming from a Trusted Host or Trusted IP address.

...unless sent from a gateway user
Enable this checkbox if you want MDaemon to permit mail relaying through domain gateways regardless of your Relay settings. This feature is disabled by default and isn't recommended.

Account Verification

SMTP MAIL address must exist if it uses a local domain
Click this option is you wish to verify that the MAIL value passed during the SMTP process points to an actual valid account when it is purported to be from a local domain or gateway.

...unless sent via authenticated SMTP session
Click this option if you wish to exempt a message from the *SMTP MAIL address must exist...* option when it is being sent via an authenticated SMTP mail session.

...unless sent from a trusted host or IP
Click this option if you wish to exempt a message from the *SMTP MAIL address must exist...* option when it is being sent from a Trusted IP address.

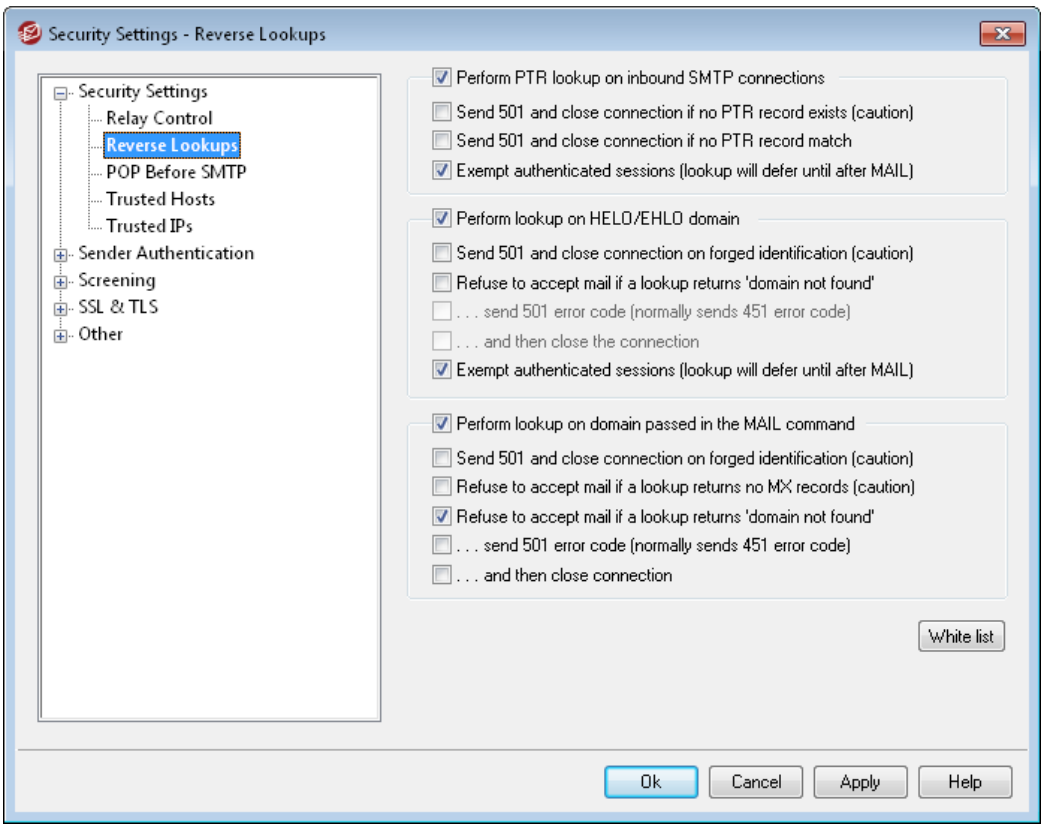
SMTP RCPT address must exist if it uses a local domain
Click this option is you wish to verify that the RCPT value passed during the SMTP process points to an actual valid account when it is purported to be from a local domain.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...unless sent via authenticated SMTP session
Click this option if you wish to exempt a message from the *SMTP RCPT address must exist...* option when it is being sent via an authenticated SMTP mail session.

...unless sent from a trusted host or IP
Click this option if you wish to exempt a message from the *SMTP RCPT address must exist...* option when it is being sent from a Trusted IP address.

4.5.1.2 Reverse Lookup


Security Settings - Reverse Lookups
Security Settings
Relay Control
Reverse Lookups
POP Before SMTP
Trusted Hosts
Trusted IPs
Sender Authentication
Screening
SSL & TLS
Other
Perform PTR lookup on inbound SMTP connections
Send 501 and close connection if no PTR record exists (caution)
Send 501 and close connection if no PTR record match
Exempt authenticated sessions (lookup will defer until after MAIL)
Perform lookup on HELO/EHLO domain
Send 501 and close connection on forged identification (caution)
Refuse to accept mail if a lookup returns 'domain not found'
. . . send 501 error code (normally sends 451 error code)
. . . and then close the connection
Exempt authenticated sessions (lookup will defer until after MAIL)
Perform lookup on domain passed in the MAIL command
Send 501 and close connection on forged identification (caution)
Refuse to accept mail if a lookup returns no MX records (caution)
Refuse to accept mail if a lookup returns 'domain not found'
. . . send 501 error code (normally sends 451 error code)
. . . and then close connection
White list
Ok
Cancel
Apply
Help

With the options on this screen, MDaemon can be configured to do a reverse lookup on the domain passed in the `HELO/EHLO` and `MAIL` commands. When performing the lookups MDaemon will attempt to acquire all of the MX and A record IP addresses for the given domain. Then the IP of the server making the connection is compared to this list in an attempt to determine whether the sender might be using a forged identity.

Oftentimes the sending mail server's IP address will not match any known MX or A records for a given domain and yet still be delivering the mail legitimately. The purpose of the Reverse Lookup process is therefore not to exclude mail but to include as much information as possible in the log files, and to provide the means whereby the postmasters can act according to their own local policies regarding these suspicious messages. To that end, an option exists that makes it possible for a special header to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

be inserted into all messages that do not pass a reverse lookup. The content filter system can then be used to determine the fate of messages containing the header.

You can also perform reverse lookups on pointer records (PTR) of incoming IP addresses. When using this option the connection can be aborted or a warning header inserted into the message if the incoming IP address does not match any PTR record.

Finally, it is generally agreed that accepting mail from sources that identify themselves by using a domain that does not exist should be optional. Therefore, a switch exists that makes it possible for you to refuse messages for which the reverse lookup process returns a "domain not found" message from the DNS server. In such cases, MDaemon will return a `451` error code, refuse to accept the message, and then allow the SMTP session to progress. However, should you wish to return a `501` error code, close the socket connection, or do both, other switches are provided for those purposes.

Trusted IP addresses and localhost (127.0.0.1) are always exempt from reverse lookups.

Perform PTR lookup on inbound SMTP connections
Enable this option if you want MDaemon to perform pointer record lookups on all inbound SMTP connections.

...send 501 and close connection if no PTR record exists (caution)
If this box is checked then MDaemon will send a `501` error code (syntax error in parameters or arguments) and close the connection if no PTR record exists for the domain.

...send 501 and close connection if no PTR record match
If this box is checked then MDaemon will send a `501` error code (syntax error in parameters or arguments) and close the connection if the result of a pointer record lookup fails to match.

Exempt authenticated sessions (lookup will defer until after MAIL)
Click this option if you wish to defer the PTR lookup on inbound SMTP connections until after the SMTP MAIL command in order to see whether or not the connection will use authentication.

Perform lookup on HELO/EHLO domain
Click this box if you want a lookup to be performed on the domain name that is reported during the `HELO/EHLO` portion of the session. The `HELO/EHLO` command is used by the client (sending machine) to identify itself to the server. The domain name passed by the client in this command is used by the server to populate the `from` portion of the `Received` header.

Perform lookup on value passed in the MAIL command
Enabling this switch will cause a lookup to be performed on the domain name that is passed during the `MAIL` command portion of the mail transaction. The address passed in the `MAIL` command is supposed to be the reverse-path for the message, and is usually the mailbox from which the message is originating. Sometimes, however, it is the address to which error messages should be directed instead.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...send 501 and close connection on forged identification (caution)
Click this check box if you want a 501 error code to be sent and then the connection closed when the result of a lookup appears to be a forged identification.

When the result of a reverse lookup states that the server is using a forged identification, this result may frequently be incorrect. It is very common for mail servers to identify themselves with values that do not match their IP addresses. This can be due to ISP limitations and restrictions and other legitimate reasons. For this reason, you should exercise caution before enabling this option. It is likely that using this option could result in your server refusing some legitimate messages.

Refuse to accept mail if a lookup returns no MX records (caution)'
Check this box if you wish to refuse MAIL from domains that do not have MX records. This option is disabled by default and should be used with caution, because domains do not need MX records in order to exist, be valid, or send/receive mail.

Refuse to accept mail if a lookup returns 'domain not found'
When a lookup results in "`domain not found`", enabling this option will cause the message to be refused with a `451` error code (Requested action aborted: local error in processing) and then the session will be allowed to progress normally to its conclusion.

...send 501 error code (normally sends 451 error code)
Enable this checkbox if you want the error code that is sent in response to a "domain not found" result to be `501` (syntax error in parameters or arguments) instead of `451`.

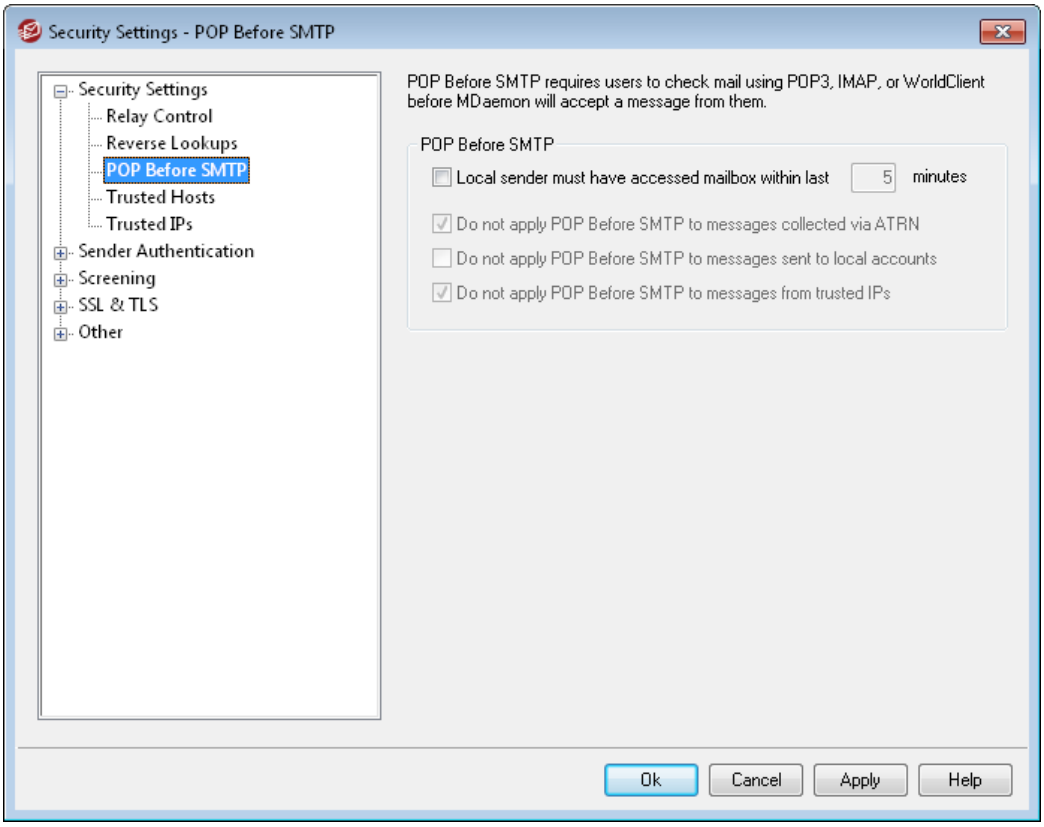
...and then close the connection
Click this checkbox if you want the connection to be closed immediately instead of allowed to progress when "`domain not found`" is the result of the reverse lookup.

Exempt authenticated sessions (lookup will defer until after MAIL)
Click this option if you wish to defer the lookup until after the SMTP MAIL command in order to see whether or not the connection will use authentication.

White list
Click this button to open the Reverse Lookup White List dialog. On it you can designate IP addresses, domains, and hosts that you wish to be exempt from reverse lookups.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.1.3 POP Before SMTP


Security Settings - POP Before SMTP
Security Settings
Relay Control
Reverse Lookups
POP Before SMTP
Trusted Hosts
Trusted IPs
Sender Authentication
Screening
SSL & TLS
Other
POP Before SMTP requires users to check mail using POP3, IMAP, or WorldClient before MDaemon will accept a message from them.
POP Before SMTP
Local sender must have accessed mailbox within last 5 minutes
Do not apply POP Before SMTP to messages collected via ATRN
Do not apply POP Before SMTP to messages sent to local accounts
Do not apply POP Before SMTP to messages from trusted IPs
Ok
Cancel
Apply
Help

POP Before SMTP

Local sender must have accessed mailbox within last [XX] minutes
With this feature enabled, whenever a message is purported to be from a local user, that user account must have logged in and checked its local mailbox within the specified number of minutes before it will be allowed to send mail.

Do not apply POP Before SMTP to messages collected via ATRN
Check this box if you want messages collected via ATRN 175 to be exempt from the POP Before SMTP restriction.

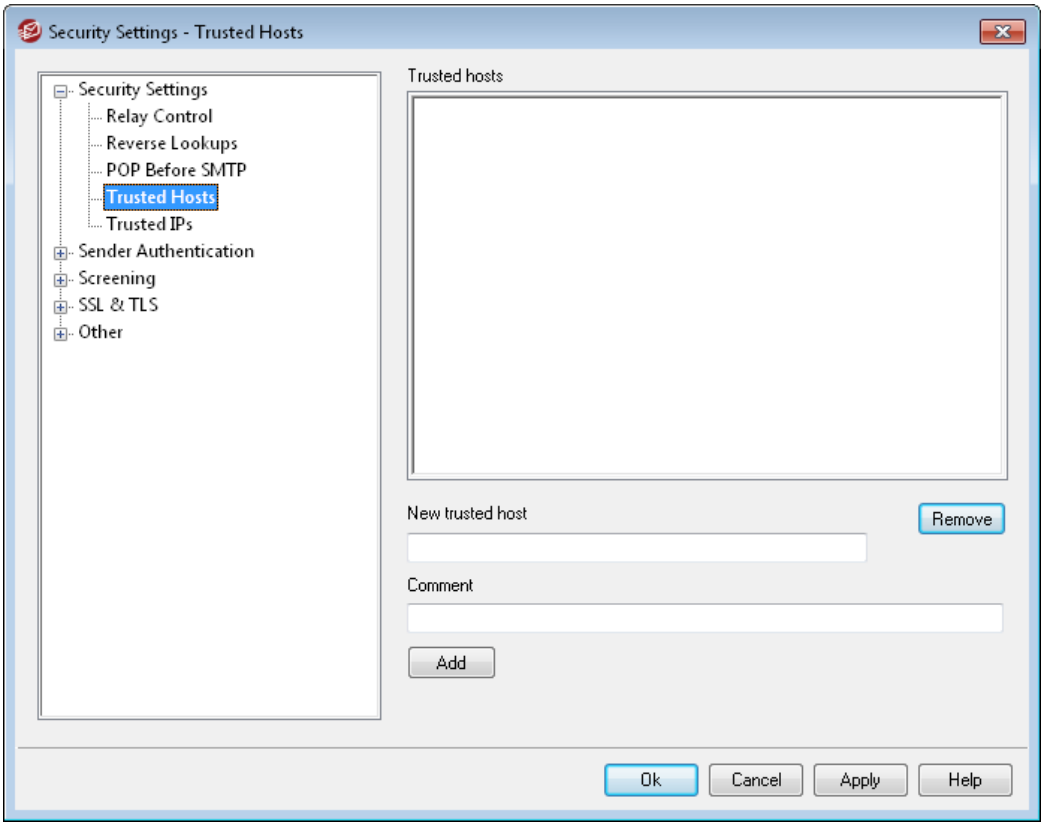
Do not apply POP Before SMTP to messages sent to local accounts
Click this checkbox if you want messages that are sent from one local user to another to be exempt from the POP Before SMTP requirement. Ordinarily, MDaemon will enforce the requirement as soon as the sender is known, but when this control is enabled MDaemon will wait until the recipient of the message is revealed before determining whether or not it is required.

Do not apply POP Before SMTP to messages from trusted IPs
If this checkbox is enabled, messages arriving from an IP address listed on the Trusted Hosts 438 screen will be exempt from POP Before SMTP.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

You can exempt authenticated sessions from the POP Before SMTP restriction via an option on the SMTP Authentication 442 screen.

4.5.1.4 Trusted Hosts



On various dialogs and security features throughout MDaemon you will see options that allow you to choose whether or not "Trusted Hosts" or "Trusted Domains" will be exceptions to or exempt from those options. The hosts you list on this screen are the ones to which those options refer.

Trusted hosts
This is the list of hosts that will be exempt from certain designated security options.

New trusted host
Enter a new host to be added to the *Trusted hosts* list.

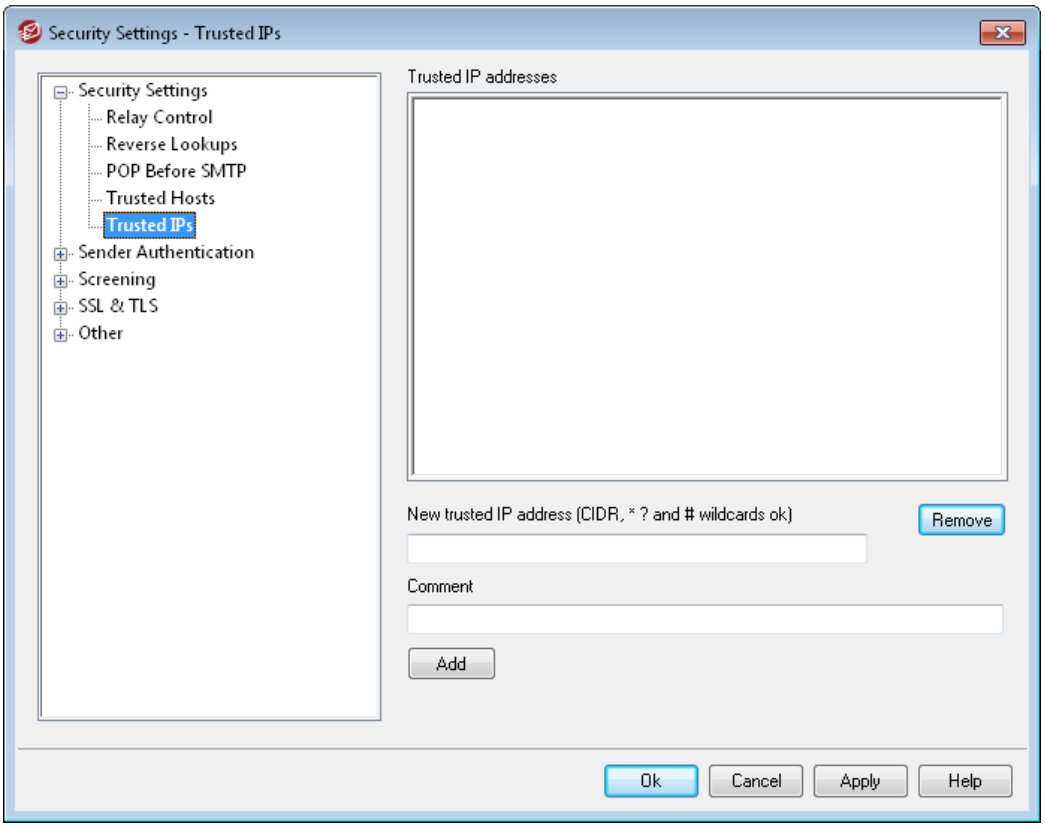
Comment
Use this for any comment text about an entry.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Add
Click this button to add the new domain to the *Trusted hosts* list.

Remove
Click this button to remove the selected entries from the *Trusted hosts* list.

4.5.1.5 Trusted IPs



On various dialogs and security features throughout MDaemon you will see options that allow you to choose whether or not "Trusted IPs" will be exceptions to or exempt from those options. The IP addresses you list on this screen are the ones to which those options refer.

Trusted IP addresses
This is the list of IP addresses that will be exempt from certain designated security options.

New trusted IP address
Enter a new IP address to be added to the *Trusted IP Addresses* list.

Comment
Use this for any comment text about an entry.

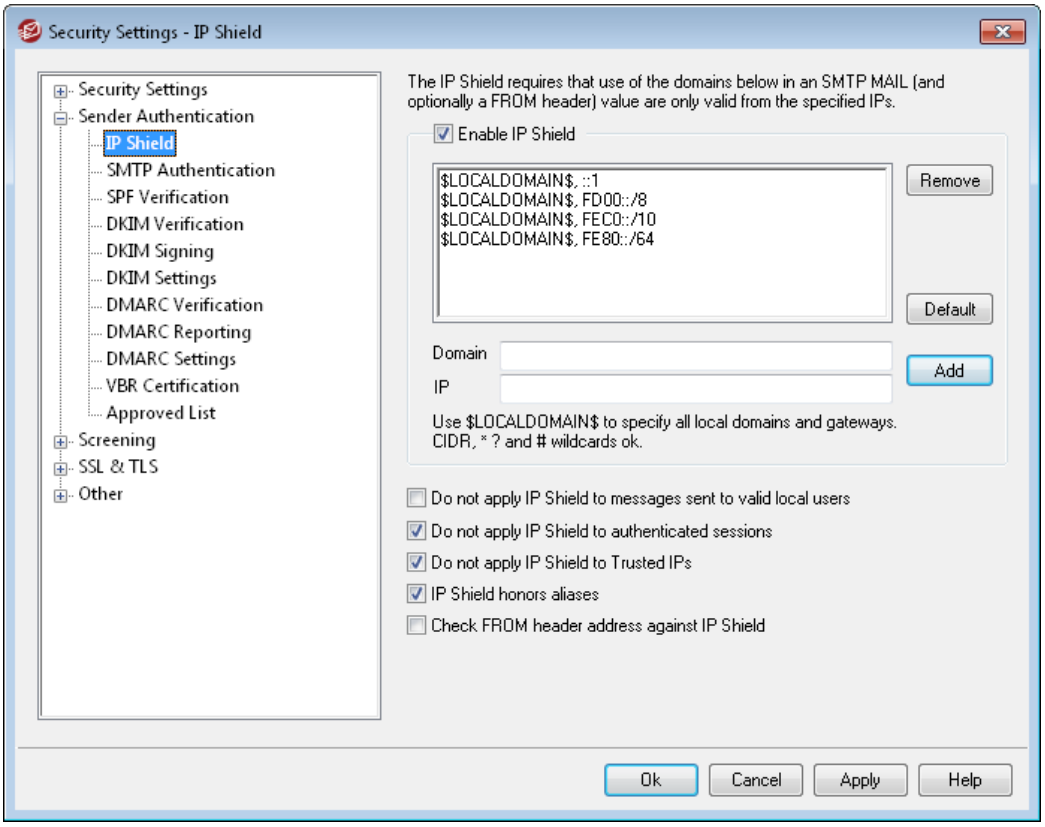
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Add
Click this button to add the new IP address to the *Trusted IP Addresses* list.

Remove
Click this button to remove the selected entries from the *Trusted IP Addresses* list.

4.5.2 Sender Authentication

4.5.2.1 IP Shield



The IP Shield, located under the Security » Security Settings menu, is a list of domain names and matching IP addresses that will be checked during the `MAIL From` command during the SMTP session. An SMTP session claiming to be from someone at one of the listed domains will be honored only if it is coming from one of the associated IP addresses. For example, suppose your domain name is example.com and your local LAN computers use IP addresses in the range from 192.168.0.0 to 192.168.0.255. With this information you can setup the IP Shield to associate the domain name example.com with the IP address range 192.168.0.* (wildcards are allowed). Thus anytime a computer connects to your SMTP server and states, "`MAIL FROM <someone@example.com>`", the SMTP session will continue only if the connecting computer has an IP address within the required range from 192.168.0.0 to 192.168.0.255.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Enable IP Shield

Clear this checkbox if you wish to disable the IP Shield. The IP Shield is enabled by default.

Domain name
Enter the domain name that you wish to associate with a specific IP address range. You can also use the `$LOCALDOMAIN$` macro to cover all local domains (including gateways). If you use this macro it will not be necessary to keep the IP Shield up to date when local domains or gateways change. By default, entries are added to the IP Shield associating all reserved IP address ranges with `$LOCALDOMAIN$`.

IP address
Enter the IP address that you wish to associate with a domain name. You must enter this address in dotted decimal form.

Add
Click the *Add* button to add the domain and IP address range to the listing.

Remove
Click this button to remove the selected entries from the listing.

Do not apply IP Shield to messages sent to valid local users
Click this option if you want only those messages that are destined for a non-local user or invalid local user to be checked for a domain/IP match. This will prevent others from posing as one of your local users in order to relay their mail through your server, but it will save resources by not checking messages that are addressed to your users. If you enable both this option and the *IP Shield honors aliases* option below, messages to valid aliases will be accepted as well.

Do not apply IP Shield to authenticated sessions
When this control is active, the IP Shield restrictions will not apply to authenticated users. Mail will be accepted from an authenticated user regardless of the IP address from which he or she connects. Further, when a user doesn't authenticate and access is refused, the message returned to the SMTP client will be "Authentication required" in order to give the user a clue that he can fix the problem by configuring the mail client to use authentication before sending a message. This option is enabled by default.

Do not apply IP Shield to Trusted IPs
When this control is active, the IP Shield will not be applied when the connection is from a Trusted IP address 438. This option is enabled by default.

IP Shield honors aliases
Enable this option if you want the IP Shield to honor address aliases when checking domain/IP address shields. The IP Shield will translate an alias to the true account to which it points and thus honor it if it passes the shield. Without this option enabled, the IP Shield will treat each alias as if it is an address independent of the account that it represents. Thus, if an alias' IP address violates an IP Shield then the message will be refused. This option is mirrored on the Settings screen 615 of Aliases — changing the setting here will be reflected there.

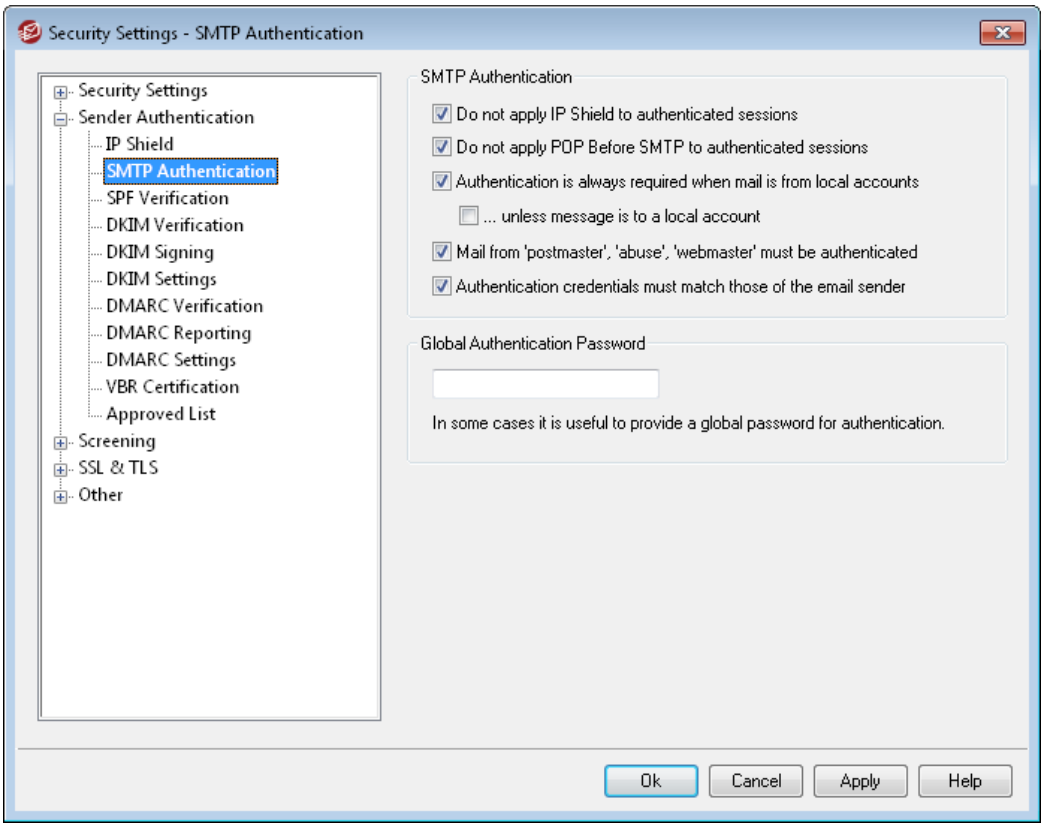
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

If you want incoming messages that are addressed to valid aliases to be exempt from IP Shielding then click both this option and the *Do not apply IP Shield to messages sent to valid local users* option above.

Check FROM header address against IP Shield
Check this box if you want the IP Shield to compare the address taken from the message's FROM header in addition to that taken from the SMTP MAIL value. This option is disabled by default.

> Using this option could cause problems with certain types of messages, such as those coming from mailing lists. It should therefore be enabled only if you are sure you need it.

4.5.2.2 SMTP Authentication



SMTP Authentication

Do not apply IP Shield to authenticated sessions
When this control is active, the IP Shield 440 restrictions will not apply to authenticated users. Mail will be accepted from an authenticated user regardless of the IP address from which he or she connects. Further, when a user doesn't authenticate and access is refused, the message returned to the SMTP client will be

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

"Authentication required" in order to give the user a clue that he can fix the problem by configuring the mail client to use authentication before sending a message. This option is enabled by default.

Do not apply POP Before SMTP to authenticated sessions
If you are utilizing the POP Before SMTP 437 security feature, you can click this option to make authenticated users exempt from this restriction. An authenticated user will not need to check his or her email before sending messages.

Authentication is always required when mail is from local accounts
When this option is enabled and an incoming message claims to be from one of MDaemon's domains, the account must first be authenticated or MDaemon will refuse to accept the message for delivery. This option is enabled by default.

> **...unless message is to a local account**
> If you are requiring authentication when a message is from a local sender, but wish to skip the authentication restriction when the recipient is local as well, then click this option. Note: this may be necessary in some situations where you require some of your users to use different mail servers for outgoing and incoming mail.

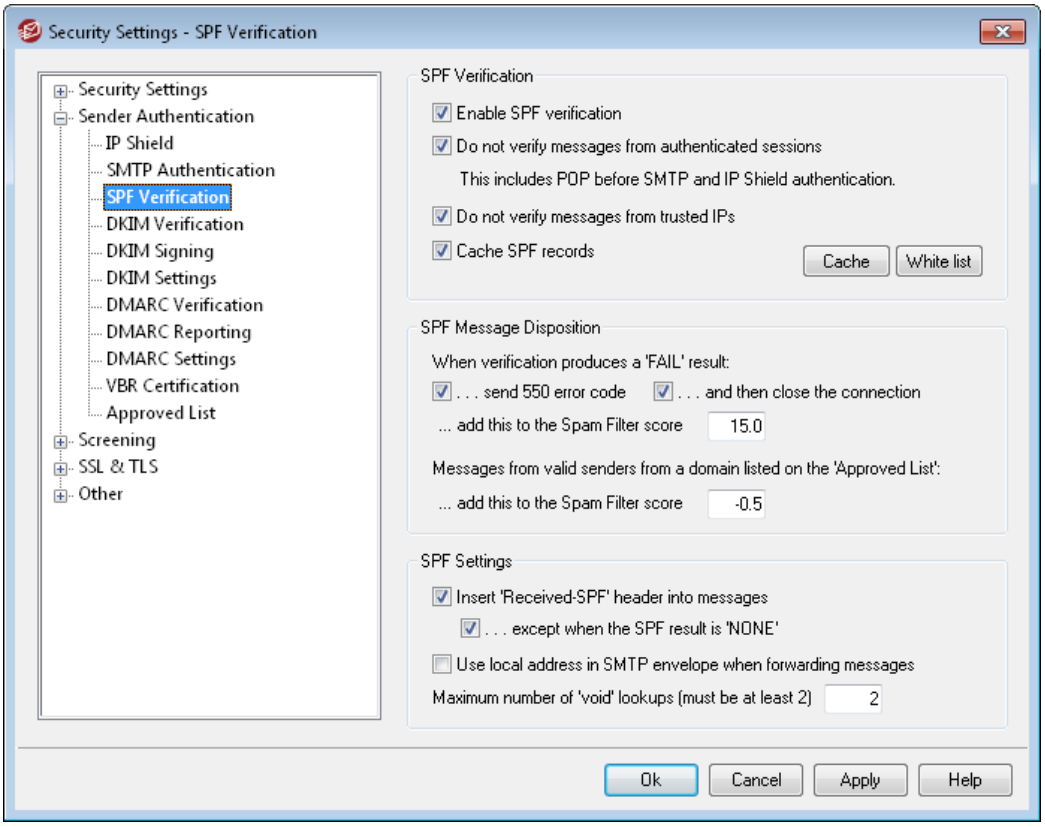
Mail from 'Postmaster', 'abuse', 'webmaster' must be authenticated
Click this checkbox to require messages claiming to be from one of your "postmaster@...", "abuse@..." or "webmaster@..." aliases or accounts to be authenticated before MDaemon will accept them. Spammers and hackers know that these addresses might exist, and may therefore attempt to use one of them to send mail through your system. This option will prevent them and other unauthorized users from being able to do so. This option is mirrored on the Settings screen 615 of Aliases. Changing the setting here will change it there as well.

Authentication credentials must match those of the email sender
Use this option if you wish to require a sender to use only his own credentials for authentication. So, for example, *user1@example.com* would only be allowed to authenticate using the *user1@example.com* account credentials. If he attempted to authenticate using *user2@example.com* then it would not be allowed, even if the *user2@example.com* credentials were valid. This option is enabled by default.

Global Authentication Password
Some configurations may require a global authentication password. If you require that then designate that password here.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.2.3 SPF Verification



MDaemon supports Sender Policy Framework (SPF) to help verify sending servers and protect against spoofing and phishing, which are two common types of email forgery in which the sender of the message attempts to make the message appear to be coming from someone else.

Many domains publish MX records in the Domain Name System (DNS) to identify the locations permitted to receive mail for them, but this doesn't identify the locations allowed to *send* mail for them. SPF is a means whereby domains can also publish sender records to identify those locations authorized to send messages. By performing an SPF lookup on incoming messages, MDaemon can attempt to determine whether or not the sending server is permitted to deliver mail for the purported sending domain, and consequently determine whether or not the sender's address may have been forged or "spoofed".

Use the options on this screen to configure your server's SPF settings.

For more information on SPF, visit:

http://spf.pobox.com

SPF Verification

Enable SPF verification
When this option is enabled, MDaemon will perform a DNS query for SPF record data on each incoming message's purported sender, to ensure that the sending server is

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

permitted to send messages on its behalf. The host MDaemon will verify is taken from the `MAIL` value passed during SMTP processing. SPF verification is enabled by default.

Do not verify messages from authenticated sessions
By default authenticated connections are exempt from SPF queries. Authenticated sessions include those verified via SMTP Authentication 442, POP before SMTP 437, or the IP Shield 440. Disable this option if you do not wish to exempt authenticated sessions from SPF.

Do not verify messages from trusted IPs
By default any message from a trusted IP address 439 is exempt from SPF verification.

Cache verification results
By default MDaemon will temporarily cache each domain's SPF policy record obtained during the DNS query. Clear the checkbox if you do not wish to cache SPF policies.

Cache
This button opens the SPF cache, which lists all currently cached SPF records.

White List
Click this button to open the SPF white list on which you can designate IP addresses that you wish to exempt from SPF lookups.

SPF Message Disposition

When verification produces a FAIL result:

...send 550 error code
Click this check box if you want a 550 error code to be sent when the result of the SPF query is "Fail".

...and then close the connection
Enable this option if you want the connection to be closed immediately after sending the 550 error code.

...add this to the Spam Filter score
Specify the amount that you wish to add to the message's Spam Score when it fails to pass SPF verification.

Messages from valid sender from a domain listed on the 'Approved List'

...add this to the Spam Filter score
Specify the amount that you wish to add to a message's Spam Score when SPF confirms that it originated from a domain found on the Approved List 474.

Ordinarily the value specified here should be a negative number so that the spam score will be reduced for the approved

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

messages.

SPF Settings

Insert 'Received-SPF' header into messages
Click this option if you want a "Received-SPF" header to be inserted into each message.

...except when the SPF result is 'NONE'
Enable this option if you do not wish the "Received-SPF" header to be inserted into a message when the result of the SPF query is "none".

Use local address in SMTP envelope when forwarding messages
Click this option if you want all mail forwarded by MDaemon to use a local address in the SMTP envelope. This helps reduce problems associated with forwarding. Normally, forwarded messages are sent using the email address of the original sender and not the email address that is actually doing the forwarding. In some situations, using a local address may be necessary in order to prevent the receiving server from falsely identifying the forwarded message as having a "spoofed" address.

Maximum number of 'Void' lookups (must be at least 2)
This is the maximum number of void lookup results permitted in an SPF query before MDaemon generates a permanent error. A Void lookup is one that results in "domain does not exist" or "no answers exist." This value must be a least "2".

4.5.2.4 DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) is a cryptographic email verification system that can be utilized to prevent spoofing (forging another person's email address in order to pose as a different message sender). Additionally, because most junk email (spam) messages contain spoofed addresses, DKIM can help greatly in the reduction of spam even though the specifications weren't specifically designed to be an anti-spam tool. DKIM can also be used to ensure the integrity of incoming messages, or ensure that the message hasn't been tampered with between the time it left the signing mail server and arrived at yours. In other words, with DKIM cryptographic verification the receiving server can be certain that the arriving message is from the server that signed it, and that no one changed that message in any way.

In order to ensure the validity and integrity of messages, DKIM uses a public and private key-pairs system. An encrypted public key is published to the sending server's DNS records and then each outgoing message is signed by the server using the corresponding encrypted private key. For incoming messages, when the receiving server sees that a message has been signed, it will retrieve the public key from the sending server's DNS records and then compare that key with the message's cryptographic signature to determine its validity. If the incoming message cannot be verified then the receiving server knows it contains a spoofed address or has been tampered with or changed. A failed message can then be rejected, or it can be accepted but have its spam score adjusted.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

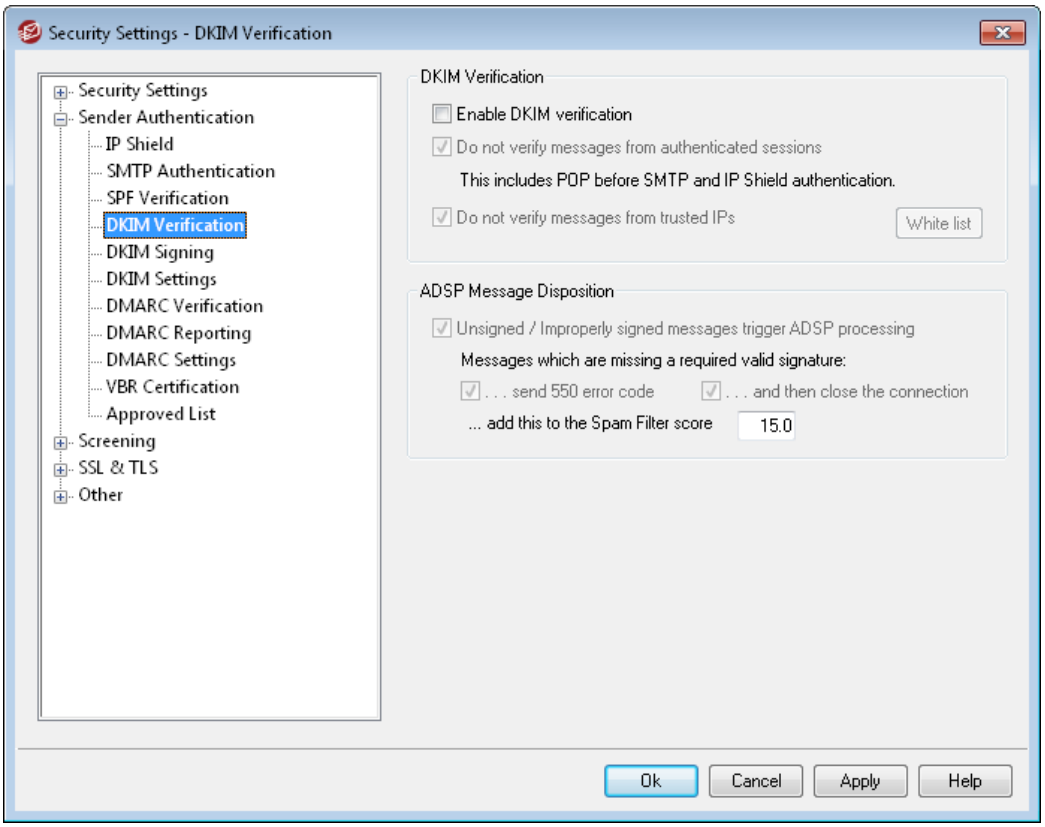
To configure MDaemon to verify incoming cryptographically signed messages, use the options provided on the DKIM Verification 447 screen. To configure MDaemon to sign outgoing messages, use the options provided on the DKIM Signing 450 screen. Both are located under the Sender Authentication section of the Security Settings dialog, at: Security » Security Settings » Sender Authentication. MDaemon's main interface 40 includes a "DKIM" tab (located under the Security tab) that can be used for monitoring DKIM activity in real time, and you can log DKIM activity using the option at: Setup » Server Settings » Logging » Settings.

See:

DKIM Verification 447
DKIM Signing 450
DKIM Settings 453

For more on DomainKeys Identified Mail, visit: http://www.dkim.org/.

4.5.2.4.1 DKIM Verification



Use this screen to configure MDaemon to verify DomainKeys Identified Mail (DKIM) signatures in incoming remote messages. When this feature is enabled and an incoming message has been cryptographically signed, MDaemon will retrieve the public key from

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

the DNS record of the domain taken from the signature and then use that key to test the message's DKIM signature to determine its validity.

If the signature passes the verification test, the message will continue on to the next step in the regular delivery process. Additionally, if the domain taken from the signature also appears on the Approved List 474, the message's Spam Filter score will receive a beneficial adjustment.

If a message has no signature, or if the signature is invalid, MDaemon will query DNS for the Author Domain Signing Practices (ADSP) record of the domain in the `From` header to determine whether or not all of that domain's messages should be signed. If the ADSP record indicates that a valid signature is required and the public key indicates that the signer is not merely testing DKIM, the message will receive a "Fail" result and be treated accordingly—it can be rejected outright or accepted but have its Spam Filter score adjusted upward.

Finally, if a site's ADSP record uses a syntax unknown to MDaemon, if no record exists at all, or if the *ADSP Message Disposition* option below is disabled, then no punitive measures will be taken. The unsigned or invalidly signed message will be treated as if the domain signs only some of its messages.

For more on DKIM see: http://www.dkim.org/

DKIM Verification

Enable DKIM verification
Click this option to enable DomainKeys Identified Mail verification of incoming remote messages. This option is required if you have SecurityPlus for MDaemon installed and wish to use its Urgent Updates 386 feature.

Do not verify messages from authenticated sessions
Click this option if you want to exempt messages from cryptographic verification when the message session is authenticated. Authenticated sessions include those verified via SMTP Authentication 442, POP before SMTP 437, or the IP Shield 440.

Do not verify messages from trusted IPs
Use this option if you want connections from trusted IP addresses 438 to be exempt from DKIM verification.

White list
Click this button to open the exception list. Messages originating from any IP addresses specified on the list will not be subject to cryptographic verification.

ADSP Message Disposition

Unsigned/Improperly signed messages trigger ADSP processing
Enable this option if you wish to query for and honor Author Domain Signing Practices (ADSP) records when an incoming message is unsigned or improperly signed. If this option is disabled or if the ADSP record uses a syntax unknown to MDaemon, then the message will be treated as if the domain signs only some of its messages.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Messages which are missing a required valid signature:

...send 550 error code
When the ADSP record indicates that a valid signature is required, any message without one will be rejected—MDaemon will return the 550 code and reject the message during the SMTP process. If, however, the signer's public key indicates that the signer is merely testing DKIM, the message will be processed normally.

...and then close the connection
Click this option if you wish to close the connection to the sending server when a message is rejected according to the previous option. If this option is disabled then the message will still be rejected according to the previous option but the connection will be allowed to continue.

...add this to the Spam Filter score
When the ADSP record indicates that a valid signature is required, any message without one will have this value added to its Spam Filter score. If, however, you have enabled the "*...send 550 error code*" option above, the message will be rejected as invalid without having to be processed through the Spam Filter. In all cases, if the signer's public key indicates that the domain is "testing," no action will be taken—the Spam Filter score will not be modified.

Using this option could still cause a message to be rejected if the resulting Spam Filter score exceeds the SMTP rejection threshold designated on the Spam Filter 402 screen.

Authentication-Results header

Whenever a message is authenticated using SMTP AUTH, SPF, DomainKeys Identified Mail, or DMARC, MDaemon will insert the Authentication-Results header into the message, listing the results of the authentication process. If MDaemon is configured to accept messages even when they fail authentication, then the Authentication-Results header will contain a code to identify the reason for the failure.

There is ongoing work via the Internet Engineering Task Force (IETF) on this header and the authentication protocols mentioned in this section. You can find more information on this at the IETF web site, located at: http://www.ietf.org/.

DKIM Headers in Mailing List Messages

By default, MDaemon strips DKIM signatures from incoming list messages because those signatures can be broken by changes made to the message headers or content during list processing. If you would like MDaemon to leave signatures in list messages, you can configure it to do so by manually setting the following option in the MDaemon.ini file:

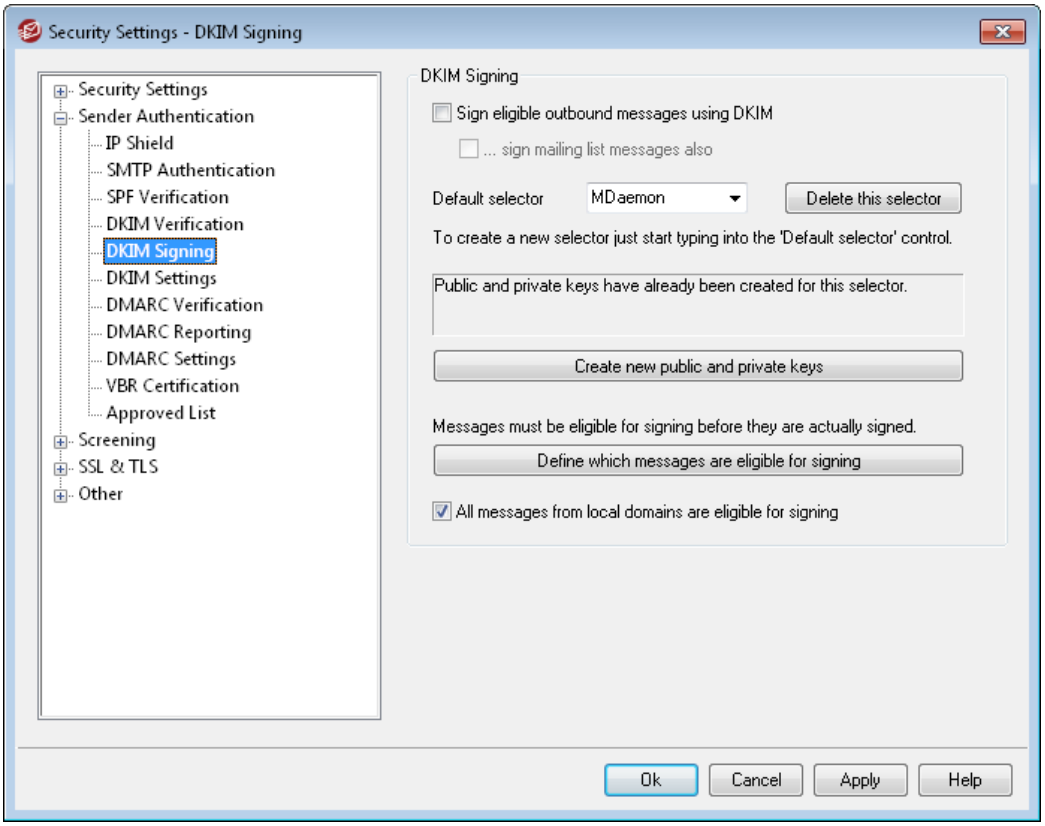
```
[DomainKeys]
StripSigsFromListMail=No (default is "Yes")
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

DomainKeys Identified Mail 446
DKIM Signing 450
DKIM Settings 453

4.5.2.4.2 DKIM Signing



Use the options contained on the DKIM Signing screen to configure MDaemon to sign eligible outbound messages using DKIM, and to define the criteria that will make a message eligible. You can also use this screen to designate selectors and generate corresponding public and private keys suitable for use with the DKIM specification. A default selector ("MDaemon") and a default public and private key are created for you automatically on startup. All keys are unique—they are never the same from one site to another, regardless of the selector specified. By default, keys are generated with a secure bit depth of 1024 bits.

DKIM Signing

Sign eligible outbound messages using DKIM
Click this option if you wish to use DomainKeys Identified Mail to cryptographically sign some outgoing messages. In order for a message to be signed, it must meet the criteria designated under the *Define which messages are eligible for signing* button and be

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

received by MDaemon for delivery on an authenticated session. There is also a Content Filter action, "*Sign with DKIM selector...*" that you can use to cause messages to be signed.

...sign mailing list messages
Click this check box if you wish to cryptographically sign all outgoing Mailing List messages. Because MDaemon will sign all mail to all of your lists, you do not need to use the "*Define which messages are eligible for signing*" option to authorize them for cryptographic signing.

Signing list mail requires content filter processing for each list message after "cracking" the list. This could affect server performance when dealing with large and highly active mailing lists.

Default selector
From the drop-down list, choose the selector whose corresponding public/private key pair you wish to use when signing messages. If you wish to create a new key pair with a different selector, type the desired selector name here and click "*Create new public and private keys*" below. If you wish to sign some messages using an alternate selector, designate a specific selector under the "*Define which messages are eligible for signing*" option, or create a Content Filter rule using the "*Sign with DKIM selector...*" action.

Delete this selector
Click this button if you wish to delete a selector. Follow the on-screen instructions that appear.

Create new public and private keys
Click this button to generate a public/private key pair for the selector specified above. A public/private key pair will be generated for the selector, and the file `dns_readme.txt` will be generated and automatically opened. This file contains example DKIM data that you will need to publish to your domain's DNS records listing your DKIM Policy and the public key for the designated selector. The file lists samples for both testing and not testing status, and for whether you are signing all messages or just some messages originating from your domain. If you are currently testing DKIM or this selector, then you will need to use the information contained in the Testing entries for either the Policy or the selector, depending on what you are testing. Otherwise you will need to use the Not Testing entries.

All keys are stored in `PEM` format, and all selectors and keys are stored under the `\MDaemon\Pem` folder in the following way:

```
\MDaemon\Pem\<Selector>\rsa.public - public key for this selector
\MDaemon\Pem\<Selector>\rsa.private - private key for this selector
```

The files contained in these folders are not encrypted or hidden, but they contain RSA private encryption keys that should never be accessed by anyone without permission. You

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

should therefore take steps to secure these folders and subfolders using your OS tools.

Define which messages are eligible for signing
If you have elected to sign eligible outbound messages, click this button to edit the `DKSign.dat` file, which contains the list of domains and addresses that MDaemon will use to determine whether or not a message should be signed. For each address listed you must designate whether or not the message should be `To` or `From` that address in order for it to qualify to be signed, or you can designate some other header such as "`Reply-To`" or "`Sender`". Optionally, you can designate a selector for each entry, which will be used when signing a message that matches that entry. Finally, you can specify an optional signing domain to be used in the "d=" tag within the signature header. This can be useful, for example, when you have multiple sub-domains signing messages. In such cases you could use the "d=" tag to tell the receiving servers to look for the DKIM keys in a single domain's DNS record, thus making it possible for you to manage all of the keys in one record rather than having to manage separate records for each sub-domain. Wildcards are permitted in domains and addresses.

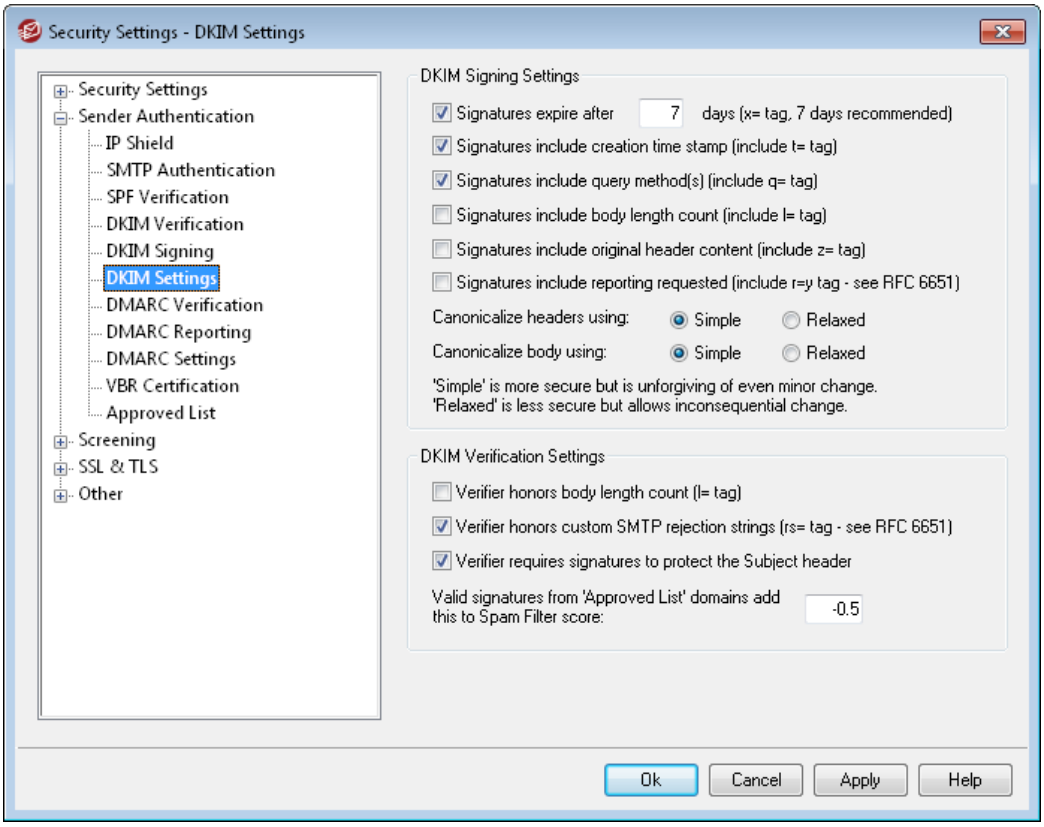
All messages from local domains are eligible for signing
Use this option if you wish to make all messages from your local domains eligible for signing. If you use this option then you do not need to add any of your local domains to the eligibility list (i.e. the `DKSign.dat` file) unless you wish to designate a specific selector or "`d=`" tag to be used when signing a specific domain's messages. This option is enabled by default.

See:

DomainKeys Identified Mail 446
DKIM Settings 453
DKIM Verification 447

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.2.4.3 DKIM Settings


Security Settings - DKIM Settings
Security Settings
Sender Authentication
IP Shield
SMTP Authentication
SPF Verification
DKIM Verification
DKIM Signing
DKIM Settings
DMARC Verification
DMARC Reporting
DMARC Settings
VBR Certification
Approved List
Screening
SSL & TLS
Other
DKIM Signing Settings
Signatures expire after 7 days (x= tag, 7 days recommended)
Signatures include creation time stamp (include t= tag)
Signatures include query method(s) (include q= tag)
Signatures include body length count (include l= tag)
Signatures include original header content (include z= tag)
Signatures include reporting requested (include r=y tag - see RFC 6651)
Canonicalize headers using: Simple Relaxed
Canonicalize body using: Simple Relaxed
'Simple' is more secure but is unforgiving of even minor change.
'Relaxed' is less secure but allows inconsequential change.
DKIM Verification Settings
Verifier honors body length count (l= tag)
Verifier honors custom SMTP rejection strings (rs= tag - see RFC 6651)
Verifier requires signatures to protect the Subject header
Valid signatures from 'Approved List' domains add this to Spam Filter score: -0.5
Ok
Cancel
Apply
Help

DKIM Signing Settings

Signatures expire after [XX] days ("x=" tag, 7 days recommended)
If you wish to limit the number of days that a DKIM signature can be considered valid, activate this option and specify the desired number of days. Messages with expired signatures will always fail verification. This option corresponds to the signature's "x=" tag. This option is enabled by default, with the value set to 7 days.

Signatures include creation time stamp (include t= tag)
When this option is enabled, the signature creation time stamp ("t=" tag) will be included in the signature. This is enabled by default.

Signatures include query method(s) (include q= tag)
By default this option is enabled. It causes the signature to include the query method tag (e.g. "q=dns").

Signatures include body length count (include l= tag)
Enable this option if you wish to include the body length count tag in DKIM signatures.

Signatures include original header content (include z= tag)
Click this option if you wish to include the "z=" tag in the DKIM signature. This tag will contain a copy of the message's original headers. This can potentially make

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

signatures quite large.

Signatures include reporting requested (include r=y tag)
Enable this option if you wish include the r=y tag in your signed messages. The presence of this tag indicates to receiving servers who honor the tag that you wish to receive AFRF failure reports from them when they encounter messages purporting to be from your domain but fail DKIM verification. To receive these reports, however, you must also configure a DKIM reporting TXT record in your domain's DNS and/or update your ADSP TXT record. See RFC-6651: *Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting*, for syntax and instructions on how to do that. Since this option requires DNS changes, it is disabled by default.

Canonicalization

Canonicalization is a process whereby the message's headers and body are converted into a canonical standard and "normalized" before the DKIM signature is created. This is necessary because some email servers and relay systems will make various inconsequential changes to the message during normal processing, which could otherwise break the signature if a canonical standard was not used to prepare each message for signing. Currently there are two canonicalization methods used for DKIM signing and verification: Simple and Relaxed. Simple is the strictest method, allowing little to no changes to the message. Relaxed is more forgiving than Simple, allowing several inconsequential changes.

Canonicalize headers using: Simple, Relaxed
This is the canonicalization method used for the message headers when signing the message. Simple allows no changes to the header fields in any way. Relaxed allows for converting header names (not header values) to lower case, converting one or more sequential spaces to a single space, and other innocuous changes. The default setting is "Simple."

Canonicalize body using: Simple, Relaxed
This is the canonicalization method used for the message body when signing the message. Simple ignores empty lines at the end of the message body—no other changes to the body are allowed. Relaxed allows for blank lines at the end of the message, ignores spaces at the end of lines, reduces all sequences of spaces in a single line to a single space character, and other minor changes. The default setting is "Simple."

DKIM Verification Settings

Verifier honors body length count (l= tag)
When this option is enabled, MDaemon will honor the body length count tag when it is found in an incoming message's DKIM signature. When the actual body length count is greater than the value contained in this tag, MDaemon will only verify the amount specified in the tag — the remainder of the message will remain unverified. This indicates that something was appended to the message, and consequently that unverified portion could be considered suspect. When the actual body length count is less than the value contained in this tag, the signature will not pass verification (i.e. it will receive a "FAIL" result). This indicates that some portion of the message was deleted, causing the body length count to be less than the amount specified in the tag.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Verifier honors custom SMTP rejection strings (rs= tag)
By default MDaemon will honor the rs= tag when it is found in an incoming message's DKIM signature. This tag allows outside domain owners to customize the SMTP rejection string that your MDaemon will display when DKIM processing results in a rejection related to their domain. Normally, this string is: "550 5.7.0 Message rejected per DKIM policy". If customized, the new string will still begin with "550 5.7.0" but the rest of the text will be replaced. The custom string cannot start with a space or number or include \r, \n, or \t. If it does, MDaemon will not replace the string. Disable this option if you do not wish to allow the string to be customized. For more information on the rs= tag, see RFC-6651: *Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting*.

Verifier requires signatures to protect the Subject header
Enable this option if you wish to require the DKIM signature of incoming messages to protect the Subject header.

Valid signatures from 'Approved List' domains add this to Spam Filter score:
The value specified here will be added to the Spam Filter score of any DKIM signed messages that receive a "Pass" result when the domain taken from the signature appears on the Approved List 474. When a message's signature is verified but the domain is not on the Approved List, the Spam Filter score will not be adjusted—the verified signature will have no effect on the score. However, normal Spam Filter processing and scoring will still be applied to that message.

Ordinarily the value specified here should be a negative number so that the spam score will be reduced for messages containing a valid cryptographic signature when the domain taken from the signature is on the Approved List 474. MDaemon's default value for this option is `-0.5`.

See:

DomainKeys Identified Mail 446
DKIM Verification 447
DKIM Signing 450

4.5.2.5 DMARC

Domain-based Message Authentication, Reporting & Conformance (DMARC) is a specification designed to help reduce email message abuse, such as incoming spam and phishing messages that misrepresent their origins by forging the message's `From:` header. DMARC makes it possible for domain owners to use the Domain Name System (DNS) to inform receiving servers of their DMARC policy, which is how they want those servers to handle messages that purport to be sent from their domain but cannot be authenticated as having actually come from it. This policy, which is retrieved by the receiving server via a DNS query while processing the incoming message, can state that the server should quarantine or reject messages that do not align with the policy, or take no action at all (i.e. let the message proceed normally). In addition to the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

policy, the domain's DMARC DNS record can also contain requests for the server to send DMARC reports to some, outlining the number of incoming messages purporting to be from that domain and whether or not they passed or failed authentication, and with details about any failures. DMARC's reporting features can be useful for determining the effectiveness of your email authentication procedures and how frequently your domain name is being used in forged messages.

Under the Sender Authentication section of the Security Settings dialog, there are three screens for configuring MDaemon's DMARC verification and reporting features: DMARC Verification, DMARC Reporting, and DMARC Settings.

DMARC Verification

As part of the DMARC verification process, MDaemon performs a DMARC DNS query on the domain found in the `From:` header of each incoming message. This is done to determine whether or not the domain uses DMARC, and if so, to retrieve its DMARC DNS record, which contains its policy and other DMARC related information. Additionally, DMARC utilizes SPF and DKIM to validate each message and requires it to pass at least one of those tests in order to pass DMARC verification. If the message passes then it will proceed normally through the rest of MDaemon's delivery and filtering processes. If it fails, however, then the fate of the message is determined by a combination of the domain's DMARC policy and how you have configured MDaemon to deal with those messages.

If a message fails DMARC verification and the DMARC domain has a policy of "`p=none`" then no punitive action will be taken and normal message processing will continue. Conversely, when the DMARC domain has a restrictive policy of "`p=quarantine`" or "`p=reject`," MDaemon can optionally filter the message automatically to the receiving user's Junk E-mail folder. You can also choose to have MDaemon reject the failed message completely when the domain is using the "`p=reject`" policy. Additionally for failed messages with restrictive policies, MDaemon will insert the "`X-MDDMARC-Fail-policy: quarantine`" or "`X-MDDMARC-Fail-policy: reject`" header, depending on the policy. This makes it possible for you to use the Content Filter to perform some action based on the presence of those headers, such as sending the message to a specific folder for further scrutiny.

DMARC Verification is enabled by default and recommended for most MDaemon configurations.

DMARC Reporting

When MDaemon queries DNS for a DMARC record, the record may contain tags indicating that the domain owner wishes to receive DMARC aggregate or failure reports regarding messages claiming to be from that domain. The options on the DMARC Reporting screen are for designating whether or not you are willing to send the requested types of reports, and for specifying the meta-data those reports should contain. Aggregate reports are sent daily at Midnight UTC and failure reports are sent per message, as each incident occurs that triggers the report. Reports are always sent as zipped XML file attachments, and there are various parsing tools available online that can make them easy for the recipients to view.

By default MDaemon does not send aggregate or failure reports. If you are willing to send either type of report, enable its corresponding options on the DMARC Reporting

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

screen.

DMARC Settings 468

The DMARC Settings screen contains various options for including certain info in DKIM reports, logging DMARC DNS records, and updating the Public Suffix file used by MDaemon for DMARC.

DMARC Verification and Mailing Lists

Because the purpose of DMARC is to ensure that the domain found in a message's `From:` header hasn't been forged, the sending server must be permitted to send messages on behalf of that domain. This can pose a unique problem for mailing lists, because it is common for lists to distribute messages on behalf of list members from outside domains, and yet leave the `From:` header unchanged. This means that when a receiving server attempts to use DMARC verification on one of these messages, the message will have been sent by a server that is not officially affiliated with the `From:` header domain. If the DMARC domain happens to be using a restrictive DMARC policy, this could cause the message to be quarantined or even rejected by the receiving server. In some cases this could also cause the recipient to be removed from the list's membership. To circumvent this problem, when MDaemon finds that a messages for a list is coming from a domain with a restrictive DMARC policy, MDaemon will replace the message's `From:` header with the mailing list's address. Alternatively, you can configure MDaemon to refuse to accept any message for a list when it is from a domain with a restrictive policy. This latter option would effectively make it impossible for a user from a domain with a restrictive policy to post a message to the list. The option to replace the `From:` header is located on the mailing list editor's Headers 192 screen. The option to reject messages is located on the Settings 189 screen.

Using DMARC for Your MDaemon Domains

If you would like to use DMARC for one of your own domains, meaning that you want receiving mail servers that support DMARC to use DMARC to verify messages claiming to be from you, then you must first ensure that you have created properly formatted SPF and DKIM DNS records for the domain; you must have at least one of those options working correctly to use DMARC. If you are using DKIM then you must also configure MDaemon's DKIM Signing 450 options to sign the domain's messages. Additionally, you must create a DMARC DNS record for the domain. By querying DNS for this specially formatted `TXT` record, the receiving server can determine your DMARC policy and various optional parameters such as: the mode of authentication you use, whether or not you wish to receive aggregate reports, the email address to which reports should be sent, and others.

Once you have properly configured DMARC and have begun to receive DMARC XML reports, there are a variety of online tools you can use to read those reports and diagnose any potential problems. For your convenience there is also a DMARC Reporter tool provided for you in the \MDaemon\App\ folder. See DMARCReporterReadMe.txt for instructions on how to use it.

Defining a DMARC TXT Resource Record

The following is an overview of the most basic, commonly used components of a DMARC record. For more detailed information, or for information on more advanced

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

configurations, see: www.dmarc.org.

Owner Field
The Owner (also called "Name" or "left-hand") field of the DMARC resource record must always be **_dmarc**, or it can take the form **_dmarc.domain.name** if you wish to specify the domain or subdomain to which the record applies.

Example:

DMARC record for the domain **example.com**

```
_dmarc IN TXT "v=DMARC1;p=none"
```
This record would apply to emails from user@example.com or any subdomains of example.com, such as user@support.example.com, user@mail.support.example.com, and so on.

```
_dmarc.support.example.com IN TXT "v=DMARC1;p=none"
```
This record would only apply to emails from user@support.example.com, not to emails from, for example, user@example.com.

```
_dmarc.support IN TXT "v=DMARC1;p=none"
```
This record would apply to emails from: user@support.example.com, user@a.support.example.com, user@a.b.support.example.com, and so on.

DMARC Record Tags and Values

Required Tags

Tag	Value	Notes
v=	**DMARC1**	The is the Version tag, which must be the first tag in the DMARC specific text portion of the record. Although other DMARC tag values are not case sensitive, the value of the **v=** tag must have the uppercase value: **DMARC1**. Example: `_dmarc IN TXT "v=DMARC1;p=none"`
p=	**none** **quarantine** **reject**	This is the Policy tag, which must be the second tag in the DMARC record, following the **v=** tag. **p=none** means that the receiving server should take no action based on results of the DMARC query. Messages that fail the DMARC check should not be quarantined or rejected based on that failure. They could still be quarantined or rejected for other reasons, such as for failing spam filter tests or other security checks unrelated to DMARC. Using **p=none** is sometimes called "monitoring" or "monitor mode" because you can use it with the **rua=** tag to receive aggregate reports from recipient domains about your

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

		messages, but those messages will not be penalized by the domains for failing to pass the DMARC check. This is the policy to use until you have thoroughly tested your DMARC implementation and are sure you are ready to move on to the more restrictive **p=quarantine** policy. **p=quarantine** is the policy to use when you want other mail servers to treat a message as suspicious when its **From:** header says that it is coming from you but the message fails the DMARC check. Depending upon the server's local policy, this could mean subjecting the message to additional scrutiny, placing it into the recipient's junk email folder, routing it to a different server, or taking some other action. **p=reject** indicates that you want the receiving server to reject any message that fails DMARC verification. Some servers, however, may still accept these message but quarantine them or subject them to additional scrutiny. This is the most restrictive policy and should generally not be used unless you have total confidence about your email policies and the types of messages or services you wish to allow your accounts to use. For example, if you wish to allow your users to join 3rd party mailing lists, use mail forwarding services, utilize "share this" features on websites, or the like, then using **p=reject** would almost certainly cause some legitimate messages to be rejected. It could also cause some users to be automatically dropped or banned from certain mailing lists. Example: `_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:dmarc-report@example.net"`

Optional Tags
All of the tags listed below are optional. When any of these tags are not used in a record then their default values are assumed.

Tag	Value	Notes
sp=	**none** **quarantine** **reject** — **Default:** If **sp=** is	This tag is for specifying a policy to be used for subdomains of the domain to which the DMARC record applies. For example, if this tag is used in a record that has scope over example.com, then the policy designated in the **p=** tag will apply to messages from example.com and the policy designated in the **sp=** tag will apply to messages from subdomains of example.com, such as mail.example.com. If this tag is omitted from the record, the **p=** tag will apply to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

	not used, the **p=** tag applies to the domain and subdomains.	the domain and its subdomains. Example: `_dmarc IN TXT "v=DMARC1;p=quarantine;sp=reject"`

rua=	Comma-separated list of email addresses to which DMARC aggregate reports should be sent. The addresses must entered as URIs in the form: **mailto:user@example.com**
	—
	Default: none
	If this tag is not used then no aggregate reports will be sent.
		This tag indicates that you wish to receive DMARC aggregate reports from servers who receive messages claiming to be **From:** a sender at your domain. Specify one or more email addresses as URIs in the form: **mailto:user@example.com**, separating multiple URIs with commas.
		Example:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:user01@example.com,mailto:user02@example.com"`
		Ordinarily these addresses will be at the domain covered by this record. If you wish to send reports to an address at some other domain, then that domain's DNS zone file must also contain a special DMARC record indicating that it will accept DMARC reports for the domain.
		Example record at example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:non-local-user@example.net"`
		Required record at example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

ruf=	Comma-separated list of email addresses to which DMARC failure reports should be sent. The addresses must entered as URIs in the form: **mailto:user@example.com**
	—
	Default: none
	If this tag is not used then no failure reports will be sent.
		This tag indicates that you wish to receive DMARC failure reports from servers who receive messages claiming to be **From:** a sender at your domain, when the conditions specified in the **fo=** tag have been met. By default, when there is no **fo=** tag specified, failure reports are sent when the message fails all DMARC verification checks (i.e. fails both SPF and DKIM). Specify one or more email addresses as URIs in the form: **mailto:user@example.com**, separating multiple URIs with commas.
		Example:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:dmarc-failures@example.com"`
		Ordinarily these addresses will be at the domain covered by this record. If you wish to send reports to an address at some other domain, then that domain's DNS zone file must also contain a special DMARC record indicating that it will accept DMARC reports for the domain.
		Example record at example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:non-local-user@example.net"`
		Required record at example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

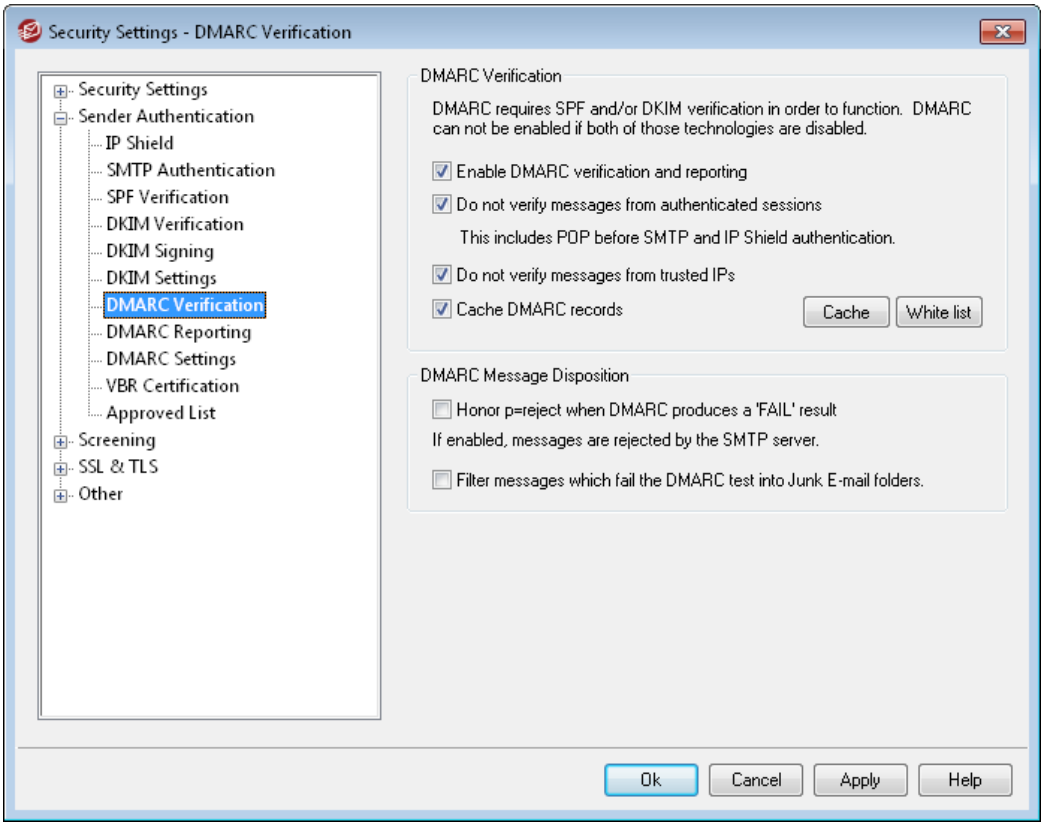
For more extensive information on the DMARC specification, see: www.dmarc.org.

See:

DMARC Verification 462
DMARC Reporting 464
DMARC Settings 468
Mailing List » Settings 189
Mailing List » Headers 192

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.2.5.1 DMARC Verification



DMARC Verification

Enable DMARC verification and reporting
When this option is enabled, MDaemon will perform DMARC DNS queries on the domain found in the `From:` header of incoming messages, and it will send aggregate and failure reports if you have set it to do son on the DMARC Reporting 464 screen. DMARC uses SPF 444 and DKIM 447 to validate messages, therefore at least one of those features must be enabled before DMARC can be used. DMARC verification and reporting is enabled by default and should be used in most MDaemon configurations.

Disabling support for DMARC could allow an increase in spam, phishing, or otherwise forged messages getting to your users. It could also cause some of your mailing list messages to be rejected by other servers and even cause some list members to be dropped from your lists. You should not disable DMARC unless you are absolutely sure that you have no need of it.

Do not verify messages from authenticated sessions
By default MDaemon will not perform DMARC queries on messages that are received over an authenticated session. Authenticated sessions include those verified by SMTP Authentication 442, POP before SMTP 437, or the IP Shield 440.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Do not verify messages from trusted IPs
By default MDaemon will not perform DMARC queries on messages that are coming from a trusted IP address 439.

Cache DMARC records
By default MDaemon will cache the DMARC record data found during the DNS lookup. By temporarily caching this information, you can increase efficiency when processing similar messages that arrive in the near future from the same domain.

Cache
This button opens the DMARC cache, which lists all currently cached DMARC records.

White list
Click this button to open the DMARC exception list. Messages originating from any IP addresses specified on the list will not be subject to DMARC verification.

DMARC Verification also honor VBR certification 471, and the Approved List 474, which can white list based on verified DKIM identifiers and SPF paths from sources you trust. So, for example, if a message arrives that fails the DMARC check but has a valid DKIM signature from a domain on the Approved List, the message is not subject to punitive DMARC policy (i.e..the message is treated as if the policy were "p=none"). The same happens if SPF path verification matches a domain on the Approved List.

DMARC Message Disposition

Honor p=reject when DMARC produces a 'FAIL' result
Enable this option if you wish to honor the `p=reject` DMARC policy when a message's `From:` domain has published that policy in its DMARC record and the message fails DMARC verification. Messages failing DMARC verification will be refused during the SMTP session.

This option is disabled by default, meaning that if the message fails DMARC verification then MDaemon will insert the "`X-MDDMARC-Fail-policy: reject`" header into the message instead of refusing to accept it. In that case you could use the Content Filter to perform some action based on the presence of that header, such as sending the message to a specific folder for further scrutiny. Further, you could use the "*Filter messages which fail the DMARC test into Junk E-mail folders*" option below to cause the message to be placed into the recipients Junk E-mail folder.

Even if you leave this option disabled, the message could still be rejected for some other reason unrelated to DMARC, such as having a Spam Filter score 402 above the permitted threshold.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

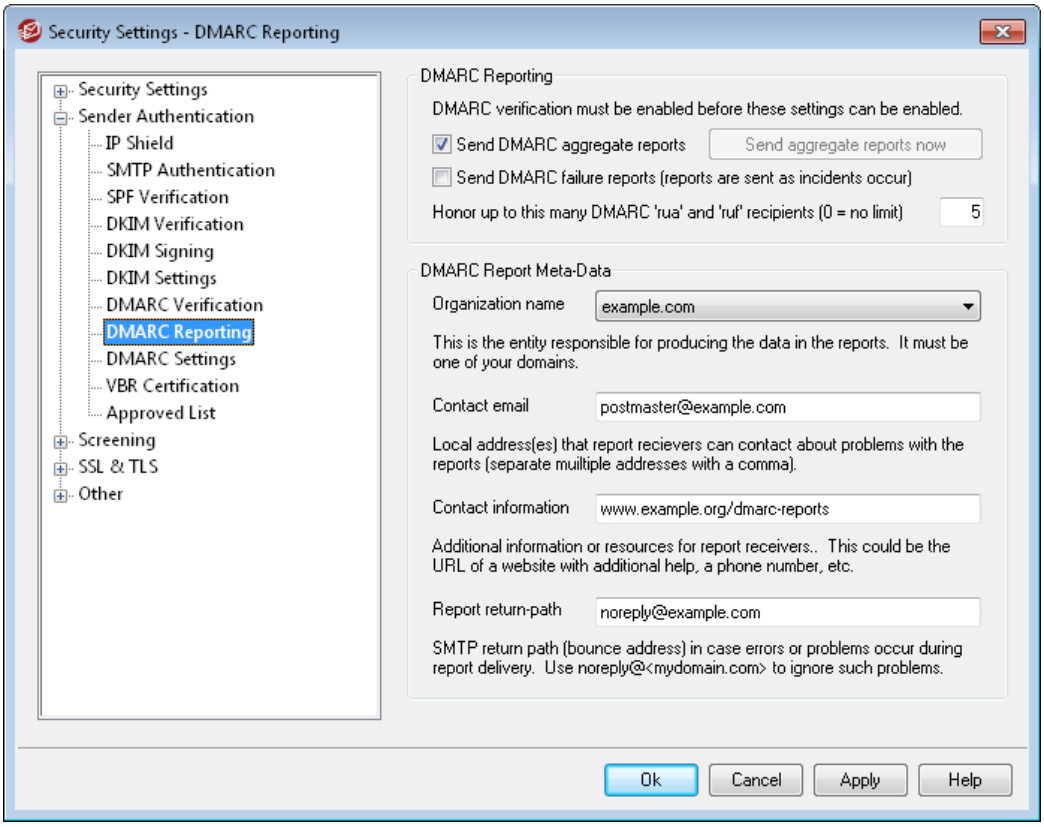
Filter messages which fail the DMARC test into Junk E-mail folders
Enable this option if you wish to filter messages automatically into the recipient account's Junk E-Mail folder whenever a message fails DMARC verification. If this folder doesn't yet exist for the user, MDaemon will create one when needed.

When enabled, this option is only applied when the From: domain has published a restrictive DMARC policy (i.e. p=quarantine or p=reject). When the domain publishes a p=none policy then that indicates that the domain is only monitoring DMARC and no punitive measure should be taken.

See:

DMARC 455
DMARC Reporting 464
DMARC Settings 468
Mailing List » Settings 189
Mailing List » Headers 192
Approved List 474

4.5.2.5.2 DMARC Reporting


Security Settings - DMARC Reporting
Security Settings
Sender Authentication
IP Shield
SMTP Authentication
SPF Verification
DKIM Verification
DKIM Signing
DKIM Settings
DMARC Verification
DMARC Reporting
DMARC Settings
VBR Certification
Approved List
Screening
SSL & TLS
Other
DMARC Reporting
DMARC verification must be enabled before these settings can be enabled.
Send DMARC aggregate reports
Send aggregate reports now
Send DMARC failure reports (reports are sent as incidents occur)
Honor up to this many DMARC 'rua' and 'ruf' recipients (0 = no limit)
5
DMARC Report Meta-Data
Organization name
example.com
This is the entity responsible for producing the data in the reports. It must be one of your domains.
Contact email
postmaster@example.com
Local address(es) that report recievers can contact about problems with the reports (separate muiltiple addresses with a comma).
Contact information
www.example.org/dmarc-reports
Additional information or resources for report receivers.. This could be the URL of a website with additional help, a phone number, etc.
Report return-path
noreply@example.com
SMTP return path (bounce address) in case errors or problems occur during report delivery. Use noreply@<mydomain.com> to ignore such problems.
Ok
Cancel
Apply
Help

When MDaemon queries DNS for a DMARC record, the record may contain various tags

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

indicating that the domain owner wishes to receive DMARC reports regarding messages claiming to be from that domain. The options on the DMARC Reporting screen are for designating whether or not you wish to send DMARC aggregate or failure reports to the domains whose DMARC records request them, and for specifying the meta-data those reports will contain. The options on this screen are only available when the "*Enable DMARC verification and reporting*" option is enabled on the DMARC Verification 462 screen. Further, the DMARC specification requires the use of STARTTLS 489 whenever it is offered by report receivers. You should therefore enable STARTTLS if possible.

DMARC Reporting

Send DMARC aggregate reports
Enable this option if you are willing to send DMARC aggregate reports to domains who request them. When a DMARC DNS query on an incoming message's `From:` domain indicates that its DMARC record contains the "`rua=`" tag (e.g. `rua=mailto:dmarc-reports@example.com`), then that means the domain owner wishes to receive DMARC aggregate reports. MDaemon will therefore store DMARC related information about the domain and about the incoming messages claiming to be from that domain. It will log the email addresses to which the aggregate report should be sent, the verification methods used for each message (SPF, DKIM, or both), whether or not the message passed or failed, the sending server, its IP address, the DMARC policy applied, and so on. Then, each day at Midnight UTC MDaemon will use the stored data to generate each domain's report and send it to the designated addresses. Once the reports are sent, the stored DMARC data is cleared and MDaemon will start the whole process again.

MDaemon does not support the DMARC report interval tag (i.e. "`ri=`") for aggregate reporting. MDaemon will send aggregate reports each day at Midnight UTC, to any domain for which it has compiled DMARC data since the last time the DMARC reports were generated and sent.

Send aggregate reports now
Click this button if you wish to generate and send a batch of aggregate reports from the currently stored DMARC data, instead of waiting until MDaemon does so automatically at the next Midnight UTC batch event. This sends the reports immediately and clears the stored DMARC data, exactly like what happens each day at Midnight UTC. MDaemon will then begin storing DMARC data again until the next Midnight UTC event, or until you click the button again, whichever come first.

Because MDaemon must be running at Midnight UTC to send aggregate reports and clear stored DMARC data automatically, if you have MDaemon shut down at that time then no reports will be generated and the DMARC data will not be cleared. DMARC data collection will continue whenever MDaemon is running again, but reports will not be generated and data will not be cleared until the next Midnight UTC event, or until you click the "*Send aggregate reports now*" button.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Send DMARC failure reports (reports are sent as incidents occur)
Enable this option if you are willing to send DMARC failure reports to domains who request them. When a DMARC DNS query on an incoming message's `From:` domain indicates that its DMARC record contains the "`ruf=`" tag (e.g. `ruf=mailto:dmarc-failure@example.com`), then that means the domain wishes to receive DMARC failure reports. Unlike aggregate reports, these reports are created in real-time as the incidents which trigger them occur, and they contain extensive detail regarding each incident and the errors that caused the failure. These reports can be used for forensic analysis by the domain's administrators to correct problems with their email system configuration or identify other problems, such as ongoing phishing attacks.

The type of failure that will trigger a failure report is dependent upon the value of the "`fo=`" tag in the domain's DMARC record. By default a failure report will only be generated if all of the underlying DMARC checks fail (i.e. both SPF and DKIM fail), but domains can use various "`fo=`" tag values to indicate that they wish to receive the reports only if SPF fails, only if DKIM fails, if either fail, or some other combination. Consequently, multiple failure reports can be generated from a single message depending upon the number of recipients in the DMARC record's "`ruf=`" tag, the value of the "`fo=`" tag, and number of independent authentication failures that are encountered for the message during processing. If you wish to limit the number of recipients to which MDaemon will send any given report, use the "*Honor up to this many DMARC 'rua' and 'ruf' recipients*" option below.

For the report format, MDaemon will only honor the `rf=afrf` tag (Authentication Failure Reporting Using the Abuse Reporting Format), which is the DMARC default. All reports are sent in this format, even if a domain's DMARC record contains the `rf=iodef` tag.

In order to support DMARC failure reporting, MDaemon fully supports: RFC 5965: An Extensible Format for Email Feedback Reports, RFC 6591: Authentication Failure Reporting Using the Abuse Reporting Format, RFC 6652: Sender Policy Framework (SPF) Authentication Failure Reporting Using the Abuse Reporting Format, RFC 6651: Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting, and RFC 6692: Source Ports in Abuse Reporting Format (ARF) Reports.

When the DMARC "`fo=`" tag requests reporting of SPF related failures, MDaemon sends SPF failure reports according to RFC 6522. Therefore, that specification's extensions must be present in the domain's SPF record. SPF failure reports are not sent independent of DMARC processing or in the absence of RFC 6522 extensions.

When the DMARC "`fo=`" tag requests reporting of DKIM related failures, MDaemon sends DKIM and ADSP failure reports according to RFC 6651. Therefore, that specification's extensions must be present in the DKIM-Signature header field, and the domain must publish a valid DKIM reporting TXT record in DNS or valid ADSP extensions in the ADSP TXT record, or

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

both. DKIM and ADSP failure reports are not sent independent of DMARC processing or in the absence of RFC 6651 extensions.

Honor up to this many DMARC 'rua' and 'ruf' recipients (0 = no limit)
If you wish to limit the number of recipients to which MDaemon will send any given DMARC aggregate report or DMARC failure report, specify the maximum number here. If a DMARC record's "rua=" or "ruf=" tag contains more addresses than your designated limit, then MDaemon will send a given report to the listed addresses, in order, until the maximum number of addresses is reached. By default there is no limit set.

DMARC Report Meta-Data

Use these options to specify your company or organization's meta-data, which will be included with the DMARC reports you send.

Organization name
This is the entity responsible for producing the DMARC reports. It must be one of your MDaemon domains. Choose the domain from the drop-down list.

Contact email
Use this option to specify local email addresses that report receivers can contact about problems with the report. Separate multiple addresses with a comma.

Contact information
Use this option to include any additional contact information for report receivers, such as a website, a phone number, or the like.

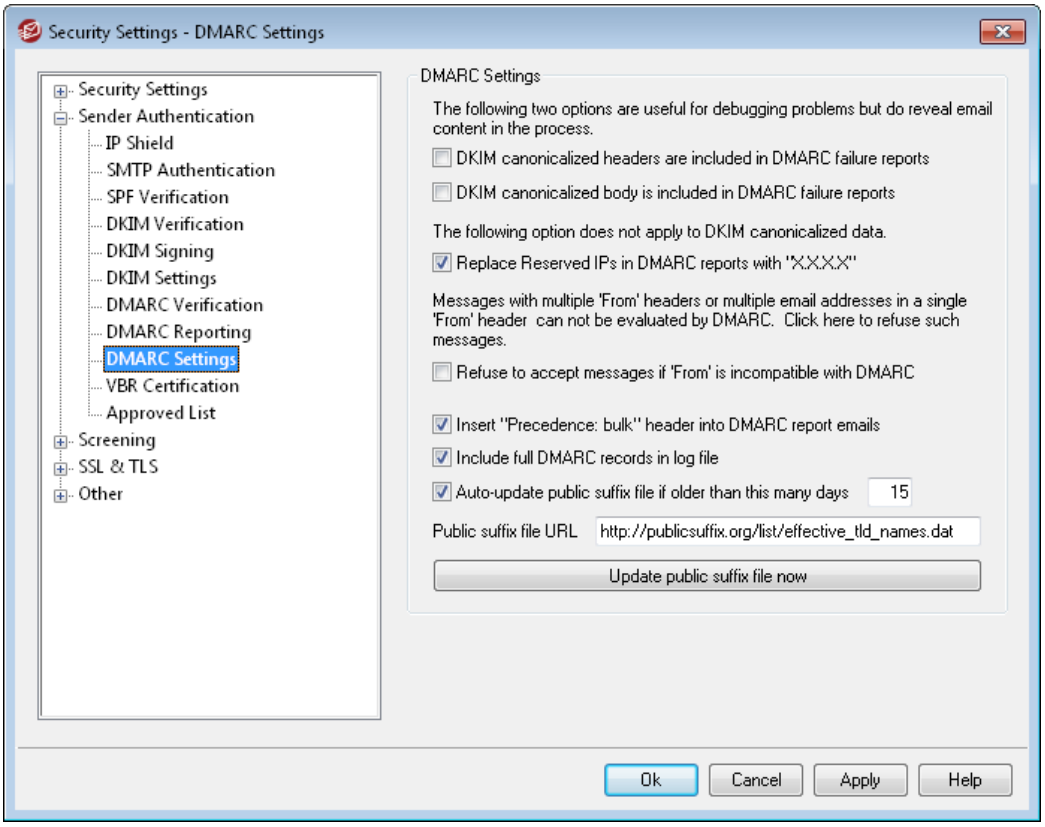
Report return-path
This is the SMTP return path (bounce address) used for report messages that MDaemon sends, in case there are delivery problems. Use noreply@<mydomain.com> to ignore such problems.

See:

DMARC 455
DMARC Verification 462
DMARC Settings 468

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.2.5.3 DMARC Settings


Security Settings - DMARC Settings
Security Settings
Sender Authentication
IP Shield
SMTP Authentication
SPF Verification
DKIM Verification
DKIM Signing
DKIM Settings
DMARC Verification
DMARC Reporting
DMARC Settings
VBR Certification
Approved List
Screening
SSL & TLS
Other
DMARC Settings
The following two options are useful for debugging problems but do reveal email content in the process.
DKIM canonicalized headers are included in DMARC failure reports
DKIM canonicalized body is included in DMARC failure reports
The following option does not apply to DKIM canonicalized data.
Replace Reserved IPs in DMARC reports with "X.X.X.X"
Messages with multiple 'From' headers or multiple email addresses in a single 'From' header can not be evaluated by DMARC. Click here to refuse such messages.
Refuse to accept messages if 'From' is incompatible with DMARC
Insert "Precedence: bulk" header into DMARC report emails
Include full DMARC records in log file
Auto-update public suffix file if older than this many days
15
Public suffix file URL
http://publicsuffix.org/list/effective_tld_names.dat
Update public suffix file now
Ok
Cancel
Apply
Help

DMARC Settings

DKIM canonicalized headers are included in DMARC failure reports
Enable this option if you wish to include DKIM canonicalized headers[453] in DMARC failure reports[464]. This is disabled by default.

DKIM canonicalized body is included in DMARC failure reports
Enable this option if you wish to include the DKIM canonicalized body[453] in DMARC failure reports[464]. This is disabled by default.

Replace Reserved IPs in DMARC reports with "X.X.X.X"
By default MDaemon replaces your reserved IP addresses in DMARC reports with "X.X.X.X". Disable this option if you wish to make your reserved IPs visible in DMARC reports. This option does not apply to DKIM canonicalized data.

Refuse to accept messages if 'From' is incompatible with DMARC
Enable this option if you wish to refuse messages that are incompatible with DMARC requirements regarding 'From' header construction. These are messages with multiple 'From' headers or multiple email addresses in a single 'From' header. Such messages are currently exempt from DMARC processing. This setting is disabled by default because having multiple addresses in a single 'From' header is not technically a protocol violation, but enabling the setting would help maximize DMARC protection. This setting is only applied when DMARC verification[462] is enabled.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Insert "Precedence: bulk" header into DMARC report emails
By default MDaemon will insert a bulk mail header into DMARC report emails. Clear this checkbox if you do not wish to insert this header.

Include full DMARC records in log file
By default MDaemon logs the full DMARC DNS record it obtains during DMARC DNS queries. Disable this option if you do not with to include the full DMARC record in the log file.

Auto-update public suffix file if older than this many days
DMARC requires a public suffix file to reliably determine the proper domains to query for DMARC DNS records. By default MDaemon will automatically update its stored public suffix file whenever it exceeds 15 days old. Change the value of this option if you wish to update the public suffix file more or less often. Disable the option if you do not wish to update it automatically.

Public suffix file URL
This is the URL of the public suffix file that MDaemon will download to use for DMARC. By default MDaemon uses the file located at: http://publicsuffix.org/list/effective_tld_names.dat.

Update public suffix file now
Click this button to manually update the public suffix file, from the *Publix suffix file URL* specified above.

See:

DMARC 455
DMARC Verification 462
DMARC Reporting 464
DKIM Settings 453

4.5.2.6 Message Certification

Message Certification is a process by which one entity vouches for or "certifies" the good email conduct of another entity. Consequently, when this certifying entity is one whom a receiving email server trusts, messages sent from a domain who is vouched for by that entity can be viewed with less suspicion. Thus the receiving server can be reasonably assured that the sending domain adheres to a set of good email practices and doesn't send spam or other problematic messages. Certification is beneficial because it can help ensure that messages will not be erroneously or needlessly subjected to unwarranted spam filter analysis. It also helps lower the resources required to process each message.

MDaemon Pro supports Message Certification by including the world's first commercial implementation of a new Internet mail protocol called "Vouch-By-Reference" (VBR), which Alt-N Technologies is working to help create and expand through its participation in the Domain Assurance Council (DAC). VBR provides the mechanism through which

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Certification Service Providers (CSP) or "certifiers" vouch for the good email practices of specific domains.

Certifying Incoming Messages

It is easy to configure MDaemon's Message Certification feature to check incoming messages. All you have to do is click the *Enable certification of inbound messages* option on the VBR Certification dialog (Security » Security Settings » Sender Authentication » VBR Certification) and include one or more certification providers whom you trust to vouch for incoming email (e.g. `vbr.emailcertification.org`). You can also choose either to exempt certified messages from spam filtering or give their Spam Filter scores a beneficial adjustment.

Certifying Outgoing Messages

Before you can configure MDaemon to insert certification data into your outgoing messages, you will first need to arrange to have one or more CSPs certify your email. Alt-N Technologies provides a certification service for MDaemon customers. For details, visit: `www.altn.com`.

To configure your MDaemon server to use Message Certification with your outgoing mail, after you have registered with a CSP:

1. Open the VBR Certification dialog: click Security » Security Settings » Sender Authentication » VBR Certification.
2. Click "*Insert certification data into outgoing messages*."
3. Click "*Configure a domain for message certification*." This opens the Certification Setup dialog.
4. Type the *Domain name* whose outgoing messages will contain the certification data.
5. Use the *Mail type* drop-down list to choose the type of email that your CSP agrees to certify for this domain, or enter a new type if the desired type isn't listed.
6. Enter one or more CSPs who will certify the domain's outbound email. If you have more than one CSP then use a space to separate each one.
7. Click "*OK*."
8. Configure your server to sign the domain's outgoing messages with DKIM 446, or ensure that they are being sent from an SPF 444 approved server. This is necessary in order to guarantee that the message originated from you. A message cannot be certified unless the receiving server can first determine that the message is authentic.

VBR does not require the certified messages to be signed by or transmitted to your CSP. The CSP is not signing or validating specific messages—it is vouching for the domain's good email practices.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

For information on the certification services provided by Alt-N Technologies, visit:

http://www.altn.com/email-certification/

VBR Specification - RFC 5518:

http://tools.ietf.org/html/rfc5518

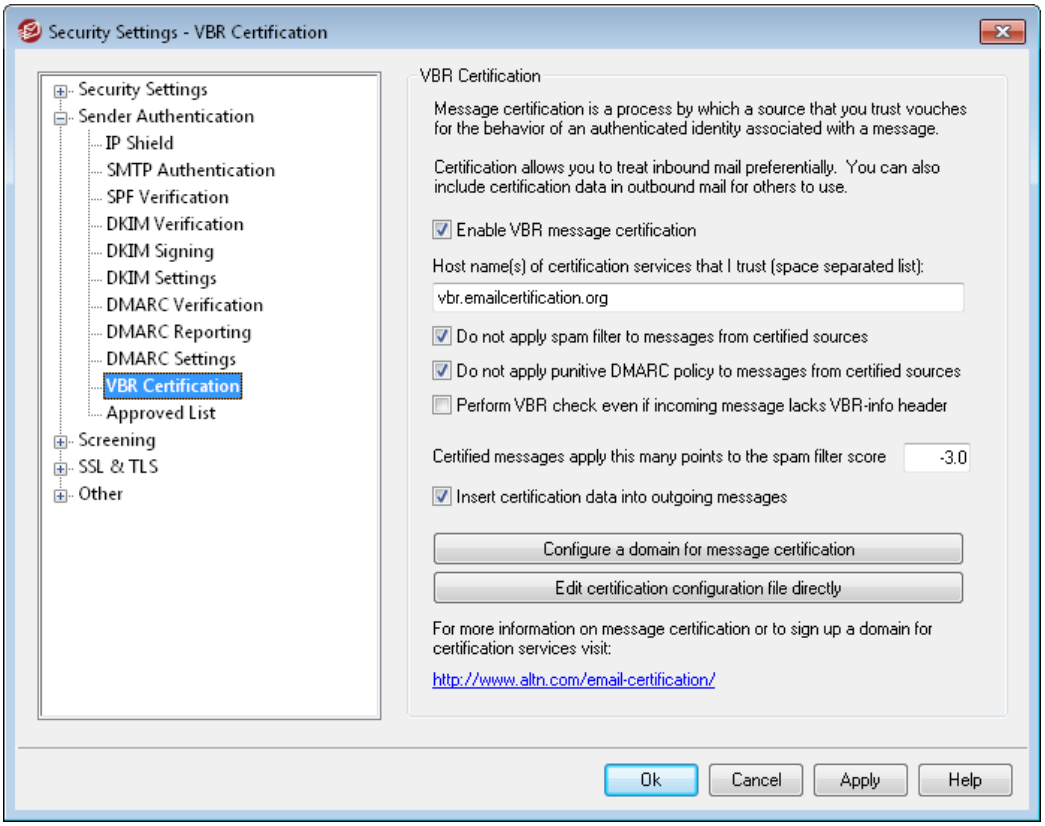
For more information on DKIM visit:

http://www.dkim.org/

See:

VBR Certification 471

4.5.2.6.1 VBR Certification


Security Settings - VBR Certification
Security Settings
Sender Authentication
IP Shield
SMTP Authentication
SPF Verification
DKIM Verification
DKIM Signing
DKIM Settings
DMARC Verification
DMARC Reporting
DMARC Settings
VBR Certification
Approved List
Screening
SSL & TLS
Other
VBR Certification
Message certification is a process by which a source that you trust vouches for the behavior of an authenticated identity associated with a message.
Certification allows you to treat inbound mail preferentially. You can also include certification data in outbound mail for others to use.
Enable VBR message certification
Host name(s) of certification services that I trust (space separated list):
vbr.emailcertification.org
Do not apply spam filter to messages from certified sources
Do not apply punitive DMARC policy to messages from certified sources
Perform VBR check even if incoming message lacks VBR-info header
Certified messages apply this many points to the spam filter score
-3.0
Insert certification data into outgoing messages
Configure a domain for message certification
Edit certification configuration file directly
For more information on message certification or to sign up a domain for certification services visit:
http://www.altn.com/email-certification/
Ok
Cancel
Apply
Help

The VBR Certification dialog is located at: Security » Security Settings » Sender Authentication » VBR Certification.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

VBR Certification

Enable VBR message certification
Click this checkbox to enable certification of inbound messages. When MDaemon receives an inbound message needing certification, it will query the trusted certification service providers (CSP) to confirm whether or not the message should actually be considered "certified." If so then the message will either be exempt from spam filtering or have its Spam Filter 401 score adjusted, depending up which option you have selected below.

Host name(s) of certification services that I trust (space separated list):
Use this box to enter the host names of the certification services that you trust. If you trust multiple services then separate each one with a space.

Do not apply spam filter to messages from certified sources
Choose this option if you want messages from certified sources to be exempt from the Spam Filter.

Do not apply punitive DMARC policy to messages from certified sources
This option ensures that verified messages from certified sources will not be penalized if the sending domain publishes a restrictive DMARC policy 462 (i.e. p=quarantine or p=reject) and the message fails the DMARC check. This option is enabled by default.

Perform VBR check even if incoming message lacks VBR-info header
Enable this option if you wish to perform VBR checks even on incoming messages that lack the VBR-Info header. Normally this header is necessary but VBR can still work without it. When the header is missing MDaemon will query your trusted CSPs using the "all" mail type. This option is disabled by default.

Certified messages apply this many points to the spam filter score
If you do not wish to exempt certified messages from spam filtering, use this option to designate the amount by which you wish to adjust the message's Spam Filter score. Ordinarily this should be a negative number so that certified messages will receive a beneficial adjustment. The default setting is "-3.0".

Insert certification data into outgoing messages
Click this checkbox to insert the certification data into outgoing messages. Then, click the *Configure a domain for message certification* button to open the Certification Setup dialog to designate the specific domains to be certified and CSPs associated with them.

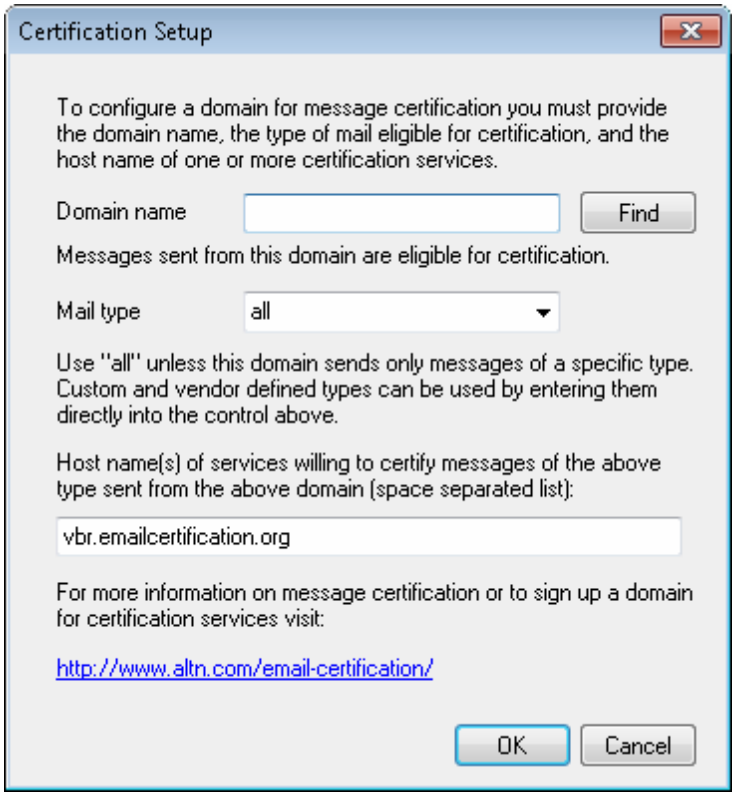
Configure a domain for message certification
After enabling the *Insert certification data into outgoing messages* option above, click this button to open the Certification Setup dialog. On this dialog you will designate the domain whose outbound messages will be certified, the types of mail that will be certified, and the CSPs associated with the domain.

Edit certification configuration file directly
After enabling the *Insert certification data into outgoing messages* option above,

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

click this button to open the Vouch-by-Reference (VBR) Configuration File. Any domains that you have configured via the Certification Setup dialog to use VBR will be listed in this file, along with the associated VBR data. You can use this file to edit those entries or manually create new entries.

Certification Setup


Certification Setup
To configure a domain for message certification you must provide the domain name, the type of mail eligible for certification, and the host name of one or more certification services.
Domain name
Find
Messages sent from this domain are eligible for certification.
Mail type
all
Use "all" unless this domain sends only messages of a specific type. Custom and vendor defined types can be used by entering them directly into the control above.
Host name(s) of services willing to certify messages of the above type sent from the above domain (space separated list):
vbr.emailcertification.org
For more information on message certification or to sign up a domain for certification services visit:
http://www.altn.com/email-certification/
OK
Cancel

After enabling the *Insert certification data into outgoing messages* option on the Certification dialog, click the *Configure a domain for message certification* button to open the Certification Setup dialog. This dialog is used to designate the domain whose outbound messages will be certified, the types of mail that will be certified, and the CSPs associated with the domain.

Certification Setup

Domain name
Use this option to enter the domain whose outbound messages will be certified.

Find
If you have previously configured the Message Certification settings for a particular domain, type the *Domain name* and then click this button and that domain's settings will be listed in the Certification Setup dialog's options.

Mail type
Use this drop-down list to choose the type of mail that the associated CSP has agreed to certify for this domain. If the type is not listed then you can type it in

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

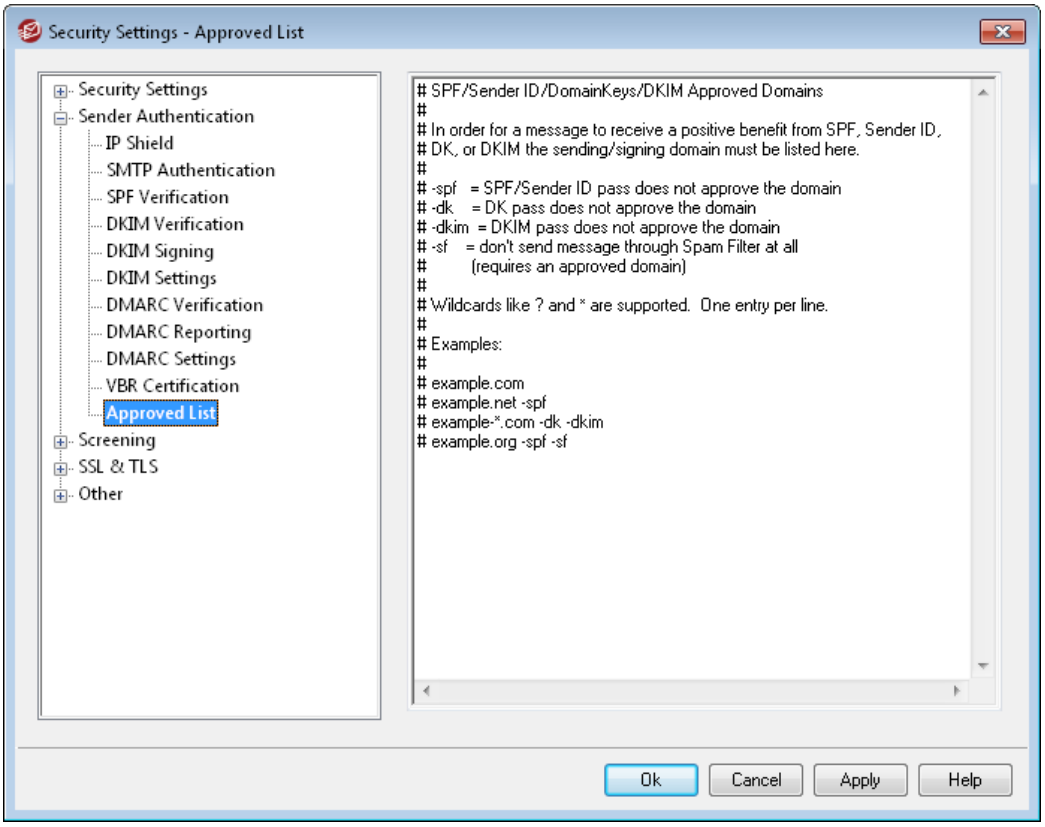
manually.

Host names(s) of services...
Enter the host names of the CSPs who have agreed to certify the domain's outbound messages (for example, `vbr.emailcertification.org`). If you enter more than one CSP then separate each one with a space.

See:

Message Certification 469

4.5.2.7 Approved List



Because some spammers and senders of bulk email have begun using SPF or signing messages with a valid DKIM signature, the fact that a message is signed and verified is no guarantee that you won't consider it to be spam, even though it does ensure that the message originated from a valid source. For this reason, a message's spam score will not be lowered as a result of SPF or DKIM verification unless the domain taken from the signature is on the Approved List. This is essentially a white list that you can use to designate domains permitted to have their messages' spam scores reduced when those incoming messages are verified.

When a message signed by one of these domains is verified by SPF or DKIM, its spam score will be reduced according to the settings found on the SPF 444 and DKIM

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Verification 447 screens. You can, however, append any of the flags listed below if you wish to prevent either of those verification methods from reducing the score. There is also a flag that you can use to prevent verified messages from being passed through the Spam Filter.

-spf Don't lower the spam score for SPF verified messages sent by this domain.

-dkim Don't lower the spam score for DKIM verified messages from this domain.

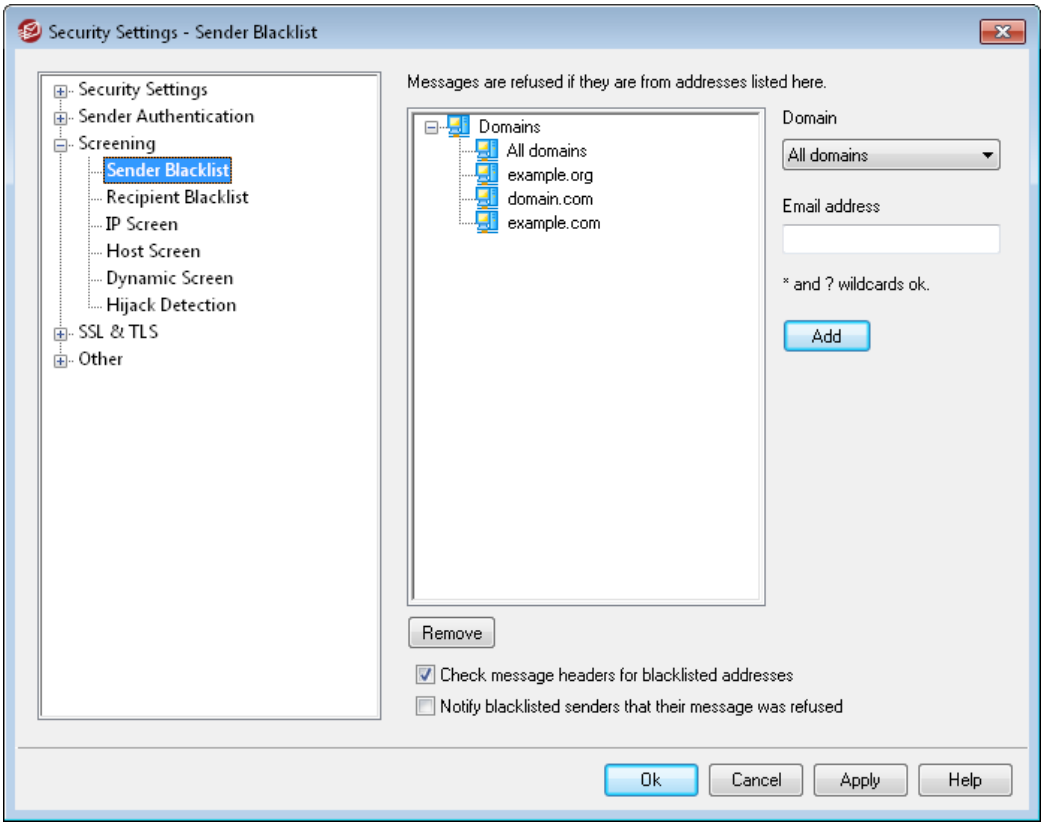
-sf Don't process verified messages from this domain through the Spam Filter.

DMARC and the Approved List

DMARC Verification 462 also utilizes the Approved List, which can white list based on verified DKIM identifiers and SPF paths from sources you trust. So, for example, if a message arrives that fails the DMARC check but has a valid DKIM signature from a domain on the Approved List, the message is not subject to punitive DMARC policy (i.e..the message is treated as if the policy were "p=none"). The same happens if SPF path verification matches a domain on the Approved List.

4.5.3 Screening

4.5.3.1 Sender Blacklist



The Sender Blacklist is located at: Security » Security Settings » Screening. This list contains addresses that are not allowed to send mail traffic through your server. If a

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

message arrives from an address on this list, it will be refused during the SMTP session. This is useful for controlling problem users. Addresses may be blacklisted on a per domain basis or globally (applied to all MDaemon domains).

Messages are refused if they are from addresses listed here
This window displays all currently blacklisted addresses, listed by the domain that is blacklisting them.

Domain
Choose the domain with which this blacklisted address will be associated. In other words, what domain do you wish to prevent from receiving mail from the specified address? Choose "All Domains" from this list to blacklist the address globally.

Email address
Enter the address that you wish to blacklist. Wildcards are accepted, therefore "*@example.net" will suppress any message from any user at "example.net", and "user1@*" will suppress any message from any address beginning with "user1@", regardless of the domain the message is from.

Add
Click this button to add the designated address to the black list.

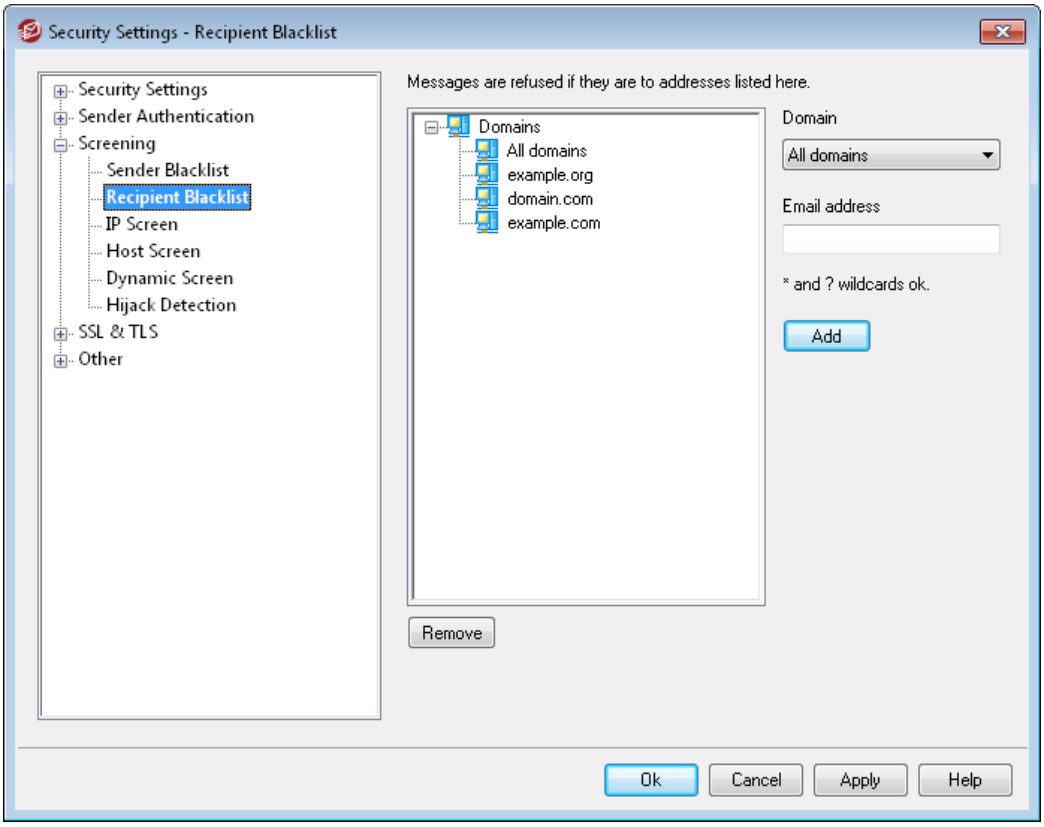
Remove
Click this button to remove an entry that you have selected in the list.

Check message headers for blacklisted senders
By default, MDaemon applies the blacklist to values taken from the message's From/ Sender header(s) during the SMTP session (after DATA completes). This prevents the message from getting caught later and moved into the bad queue by the MTA thread.

Notify blacklisted senders that their message was refused
If selected, a message will be routed back to the blacklisted sender telling him or her that the message was refused.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.3.2 Recipient Blacklist



The Recipient Blacklist is located at: Security » Security Settings » Screening. This list contains email addresses that are not allowed to receive mail through your server. If a message arrives for an address on this list, it will be refused. Addresses may be blacklisted on a per domain basis or globally (applied to all MDaemon domains). The Recipient Blacklist operates on SMTP envelope RCPT data only (not message headers).

Messages are refused if they are to addresses listed here
This window displays all currently blacklisted addresses, listed by the domain that is blacklisting them.

Domain
Choose the domain with which this blacklisted address will be associated. In other words, what domain do you wish to prevent from receiving mail for the specified address? Choose "All Domains" from this list to blacklist the address globally.

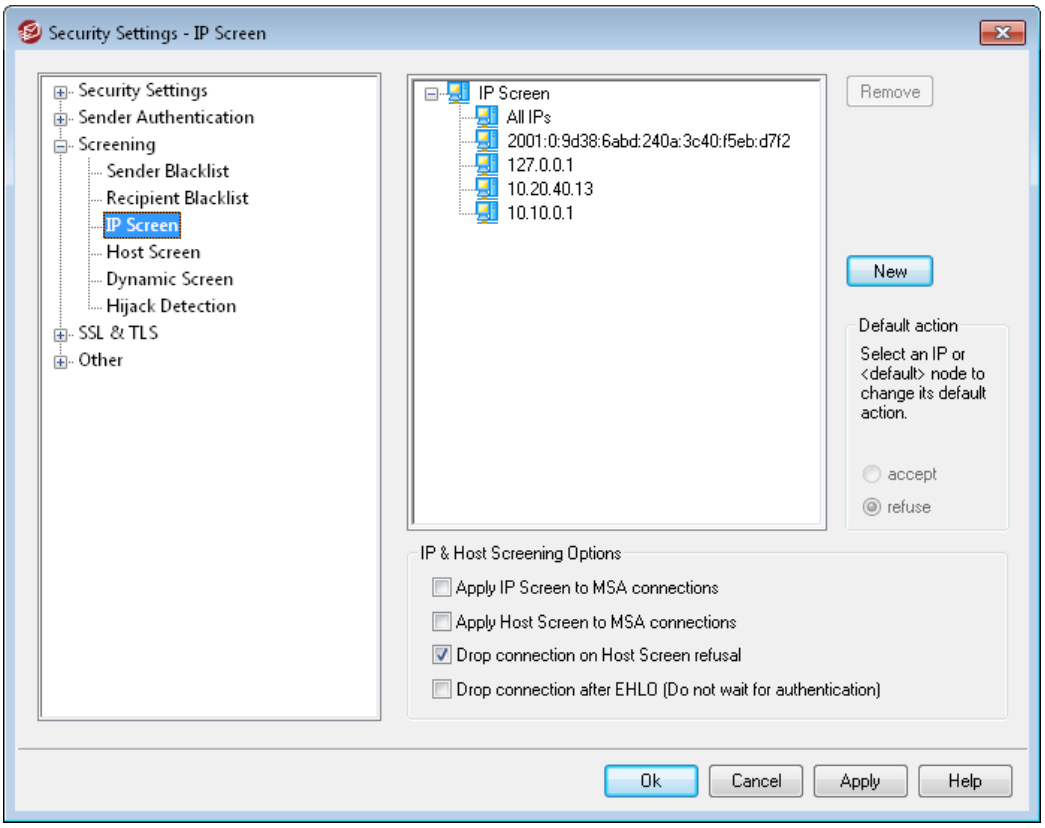
Email address
Enter the address that you wish to blacklist. Wildcards are accepted, therefore "*@example.net" will suppress any message for any user at "example.net", and "user1@*" will suppress any message for any address beginning with "user1@", regardless of the domain to which the message is addressed.

Add
Click this button to add the designated address to the black list.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Remove
Click this button to remove an entry that you have selected in the list.

4.5.3.3 IP Screen



The IP Screen is located under: Security » Security Settings » Screening. It is used to define specific remote IP addresses that will be allowed to connect, or not allowed to connect, to your local IP addresses. The remote IP addresses you place on the IP Screen can be associated with either all of you local IP addresses or with individual IPs. CIDR notation and the wildcards *, #, and ? are allowed.

For example:

..*.*	Matches to any IP address
#.#.#.#	Matches to any IP address
192.*.*.*	Matches to any IP that begins with 192
192.168.*.239	Matches to IP addresses from 192.168.0.239 to 192.168.255.239
192.168.0.1??	Matches to IP addresses from 192.168.0.100 to 192.168.0.199

New IP Screen Item

To create a new IP Screen entry, click **New**. This will open the New IP Screen Item dialog for creating the entry.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Local IP
In the drop-down list choose either "All IP's" or the specific IP to which this item will apply.

Remote IP (CIDR, * ? and # wildcards are ok)
Enter the remote IP address that you wish to add to the list, associated with the Local IP designated above.

Accept connections
Selecting this option means that the specified remote IP addresses will be allowed to connect to the associated local IP address.

Refuse connections
Selecting this option means that the specified remote IP addresses will NOT be allowed to connect to the associated local IP address. The connection will be refused or dropped.

Add
When you have finished entering the information in the options above, click this button to add the entry to the list.

Remove

To remove an entry, select the entry in the list and click **Remove**.

Default Action

To specify the default action for connections from remote IP addresses that have not been defined, select an IP address from the list and click **accept** or **refuse**. Once a default action has been specified, you can change it by selecting the "<default>" node beneath the IP address and then selecting the new default setting.

accept
When this option is chosen, connections from any IP addresses not specifically defined on the IP Screen will be accepted.

refuse
When this option is chosen, connections from any IP addresses not specifically defined on the IP Screen will be dropped, or refused.

The IP Screen will never block trusted IPs 438 or local IPs.

IP & Host Screening Options

Apply IP Screen to MSA connections
Use this option to apply IP Screening to connections made to the server's MSA port 56. Normally this is not necessary. This setting is disabled by default.

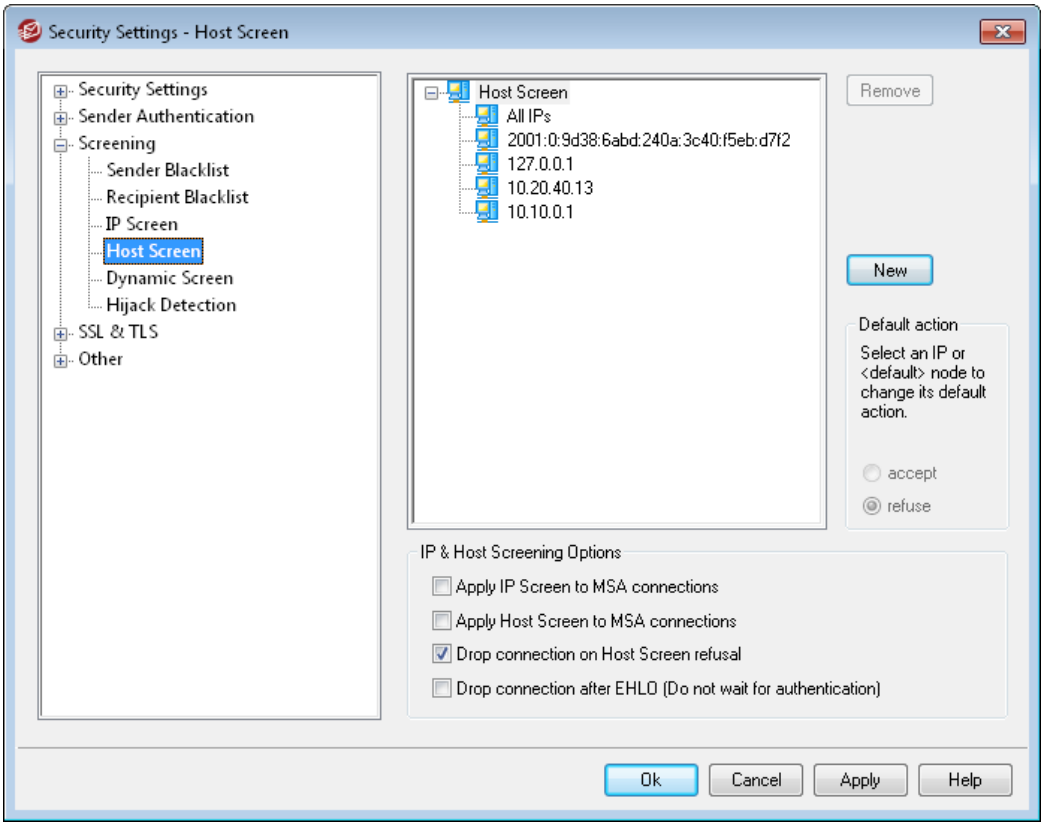
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Apply Host Screen to MSA connections
Use this option to apply Host Screening to connections made to the server's MSA port 561. Normally this is not necessary. This setting is disabled by default.

Drop connection on Host Screen refusal
When this option is enabled, the connection will be dropped immediately upon a Host Screen refusal.

Drop connection after EHLO (Do not wait for authentication)
Enable this option if you wish to drop banned connections immediately following EHLO/HELO. Normally you would wait for authentication. This setting is disabled by default.

4.5.3.4 Host Screen



The Host Screen is located at: Security » Security Settings » Screening. It is used to define which remote hosts will be allowed to connect to your local IP addresses. You may specify a list of hosts and configure the server to allow only connections from those hosts, or you can configure it to refuse connections from the listed hosts. Host screening compares the EHLO and PTR values determined during the SMTP session with the values specified here.

New Host Screen Item

To create a new Host Screen entry, click **New**. This will open the New Host Screen

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Item dialog for creating the entry.

Local IP
Use this drop-down list to choose the local IP address to which this Host Screen entry will apply. Choose "All IPs" if you wish it to apply to all of your local IP addresses.

Remote host (* and # wildcards ok)
Enter the remote host that you wish to add to the list, associated with the Local IP designated above.

Accept connections
Selecting this option means that the specified remote host will be allowed to connect to the associated local IP address.

Refuse connections
Selecting this option means that the specified remote host will NOT be allowed to connect to the associated local IP address. The connection will be refused or dropped.

Remove

To remove an entry, select the entry in the list and click **Remove**.

Default Action

To specify the default action for connections from remote hosts that have not been defined, select an IP address from the list and click **accept** or **refuse**. Once a default action has been specified, you can change it by selecting the "<default>" node beneath the IP address and then selecting the new default setting.

accept
When this option is chosen, connections from any host not specifically defined on the Host Screen will be accepted.

refuse
When this option is chosen, connections from any host not specifically defined on the Host Screen will be refused.

The Host Screen will never block trusted 438 or local hosts.

IP & Host Screening Options

Apply IP Screen to MSA connections
Use this option to apply IP Screening to connections made to the server's MSA port 56. Normally this is not necessary. This setting is disabled by default.

Apply Host Screen to MSA connections
Use this option to apply Host Screening to connections made to the server's MSA

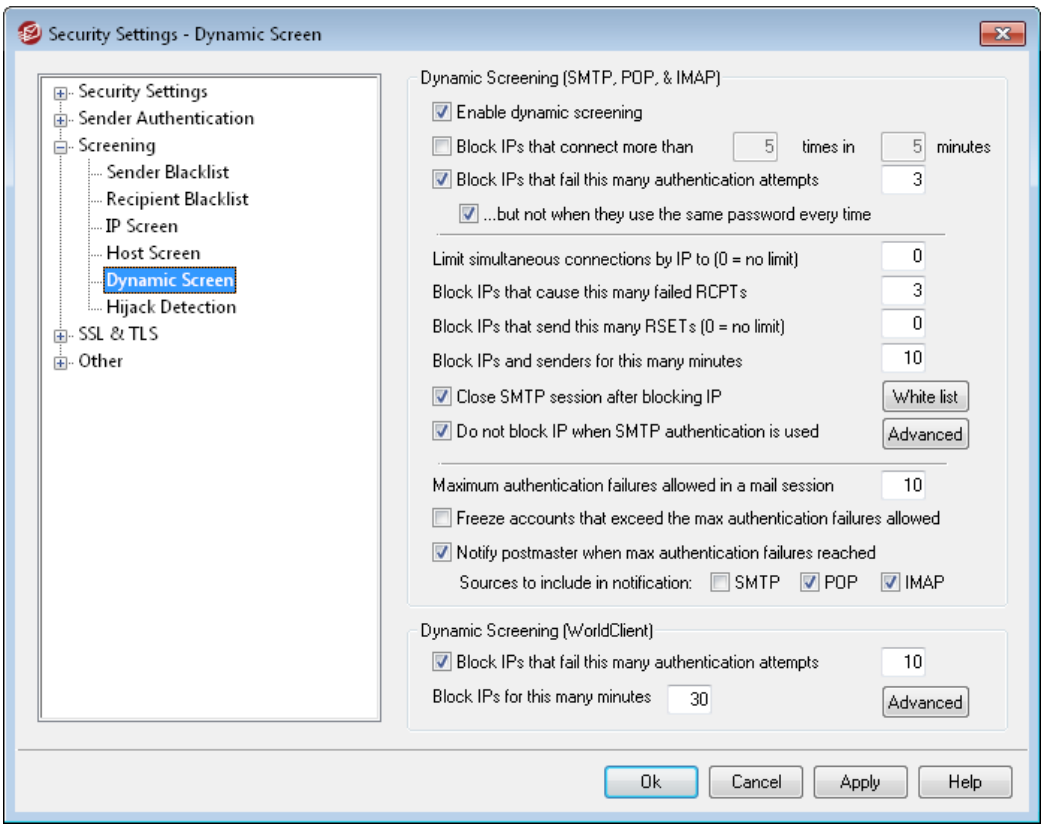
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

port 561. Normally this is not necessary. This setting is disabled by default.

Drop connection on Host Screen refusal
When this option is enabled, the connection will be dropped immediately upon a Host Screen refusal.

Drop connection after EHLO (Do not wait for authentication)
Enable this option if you wish to drop banned connections immediately following EHLO/HELO. Normally you would wait for authentication. This setting is disabled by default.

4.5.3.5 Dynamic Screen


Security Settings - Dynamic Screen
Security Settings
Sender Authentication
Screening
Sender Blacklist
Recipient Blacklist
IP Screen
Host Screen
Dynamic Screen
Hijack Detection
SSL & TLS
Other
Dynamic Screening (SMTP, POP, & IMAP)
Enable dynamic screening
Block IPs that connect more than 5 times in 5 minutes
Block IPs that fail this many authentication attempts 3
...but not when they use the same password every time
Limit simultaneous connections by IP to (0 = no limit) 0
Block IPs that cause this many failed RCPTs 3
Block IPs that send this many RSETs (0 = no limit) 0
Block IPs and senders for this many minutes 10
Close SMTP session after blocking IP
White list
Do not block IP when SMTP authentication is used
Advanced
Maximum authentication failures allowed in a mail session 10
Freeze accounts that exceed the max authentication failures allowed
Notify postmaster when max authentication failures reached
Sources to include in notification: SMTP POP IMAP
Dynamic Screening (WorldClient)
Block IPs that fail this many authentication attempts 10
Block IPs for this many minutes 30
Advanced
Ok
Cancel
Apply
Help

Using the Dynamic Screening features, MDaemon can track the behavior of sending servers to identify suspicious activity and then respond accordingly. For example, you can temporarily block an IP address from future connections to your server once a specified number of "unknown recipient" errors occur during the mail connection from that IP address. You can also block senders that connect to your server more than a specified number of times in a specified number of minutes, and senders that fail authentication attempts more than a designated number of times.

When a sender is blocked, it is not permanent. The sender's IP address will be blocked for the number of minutes that you have specified on this dialog. Blocked addresses are contained in the `DynamicScreen.dat` file. It contains a list of the blocked IP addresses and the length of time each will be blocked. This file is memory resident and

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

can be changed from the *Advanced* button. If you wish to edit or add the IP addresses manually using a text editor, you should create the `DynamicScreenUpd.sem` Semaphore File 684 and place it in MDaemon's `\APP\` folder rather than editing the `DynamicScreen.dat` file directly.

The "Dynamic screening (WorldClient)" section provides options that allow you to screen WorldClient connections.

Dynamic Screening (SMTP, POP, & IMAP)

Enable dynamic screening
Click this check box to enable dynamic screening. This option screens SMTP, POP3, and IMAP connections.

Block IPs that connect more than [X] times in [X] minutes
Click this check box if you wish to temporarily block IP addresses that connect to your server an excessive number of times in a limited time period. Specify the number of minutes and the number of connections allowed in that period.

Block IPs that fail this many authentication attempts
Use this option if you wish to temporarily block IPs that fail an authentication attempt a specified number of times. This can help prevent attempts to "hack" a user account and falsely authenticate a session. This option monitors SMTP, POP3, and IMAP connections. The database of failed authentication attempts is reset at midnight each night.

...but not when they use the same password every time
By default Dynamic Screening will not block IP addresses for failing too many authentication attempts when each of the failed attempts uses the same password. This is to prevent a legitimate client from having its IP address blocked due to the client not yet being configured with a new password. Disable this option if you wish to block an IP address even when all failed attempts used the same password.

Limit simultaneous connections by IP to (0 = no limit)
This is the maximum number of simultaneous connections allowed from a single IP address before it will be blocked. Use "0" if you do not wish to set a limit.

Block IPs that cause this many failed RCPTs
When an IP address causes this number of "Recipient unknown" errors during a mail session it will be automatically blocked for the number of minutes specified in the *Block IPs for this many minutes* option below. Frequent "Recipient unknown" errors are often a clue that the sender is a spammer, since spammers commonly attempt to send messages to outdated or incorrect addresses.

Block IPs that send this many RSETs (0 = no limit)
Use this option if you wish to block any IP address that issues the designated number of RSET commands during a single mail session. Use "0" if you do not wish to set a limit. There is a similar option on the Servers 53 screen under Server Settings that can be used to set a hard limit on the allowed number of RSET commands.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Block IPs and senders for this many minutes
When an IP address or sender is automatically blocked, this is the number of minutes the block will last. When the block expires the IP or sender will be able to send to you again normally. This feature prevents you from accidentally blocking a valid IP address or sender permanently.

Close SMTP session after blocking IP
Enabling this option causes MDaemon to close the SMTP session after the IP address is blocked.

Do not block IP when when SMTP authentication is used
Click this checkbox if you want senders who authenticate their mail sessions before sending to be exempt from Dynamic Screening.

White list
Click this button to open the Tarpit/Dynamic Screening white list. IP addresses listed there are exempt from tarpitting and dynamic screening.

Advanced
Click this button to open the `DynamicScreen.dat` block list. This lists all IP addresses that have been blocked by Dynamic Screening. You can manually add IP addresses and the number of minutes to block them by listing them one entry per line in the form: `IP_address<space>Minutes`. For example, `192.0.2.0 60`.

Maximum authentication failures allowed in a mail session
This is the maximum number of failed authentication attempts allowed in a mail session before the actions below (if any) are taken. This is set to 10 by default.

Freeze accounts that exceed the max authentication failures allowed
Check this box if you wish to freeze accounts that fail more than the designated number of authentication attempts. If an account is frozen an email is always sent to the postmaster. Replying to that email will re-enable the account.

Notify postmaster when max authentication failures reached
Check this box if you wish to send a notification email to the postmaster whenever an account fails the designated number of authentication attempts.

Sources to include in notification: SMTP, POP, IMAP
Use this option to designate the source protocols that will trigger authentication failure notifications: SMTP, POP, or IMAP. If, for example, you don't wish to be notified of SMTP authentication failures, leave the SMTP option unchecked. You would then only receive the authentication failure emails for POP and IMAP failures.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Dynamic Screening (WorldClient)

Block IPs that fail this many authentication attempts
Use this option if you wish to temporarily block IP addresses that fail a WorldClient authentication attempt a specified number of times. This can help prevent attempts to "hack" a user account and falsely authenticate a session. This option monitors only WorldClient connections.

WorldClient sends an email to the postmaster when dynamic screening bans an IP address. The following settings to control this option are located in the `WorldClient.ini` file at: `\MDaemon\WorldClient\WorldClient.ini`

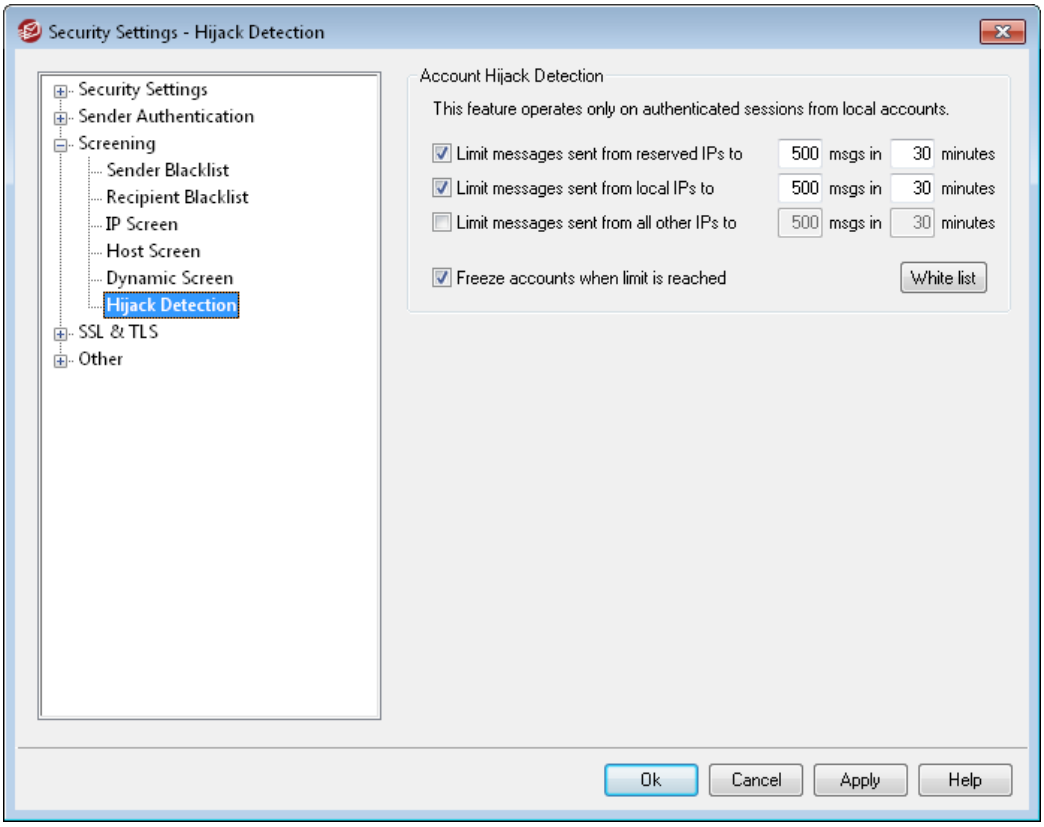
```
[DynamicScreening]
SendBanNotification=Yes
SendBanNotificationTo=postmaster
```

Block IPs for this many minutes
When an IP address is automatically blocked, this is the number of minutes the block will last. When the block expires the IP address will be able to connect to you again normally. This feature prevents you from accidentally blocking a valid IP address permanently.

Advanced
Click this button to open the Dynamic Screen's WorldClient block list. This lists all IP addresses that have been blocked from connecting to WorldClient. You can manually add IP addresses and the number of minutes to block them by listing them one entry per line in the form: `IP_address<space>Minutes`. For example, `192.0.2.0 60`.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.3.6 Hijack Detection



Account Hijack Detection

The options on this screen can be used to detect a possibly hijacked MDaemon account and automatically prevent it from sending messages through your server. For example, if a spammer somehow obtained an account's email address and password then this feature could prevent the spammer from using the account to send bulk junk e-mail through your system. You can designate a maximum number of messages that may be sent by an account in a given number of minutes, based on the IP address from which it is connecting. You can also choose to disable accounts that reach the limit. There is also a *White List* that can be used to exempt certain addresses from this restriction. Account Hijack Detection is enabled by default.

Account Hijack Detection only applies to local accounts over authenticated sessions, and the Postmaster account is automatically exempt.

Limit messages sent from reserved IPs to [xx] msgs in [xx] minutes

Use this option to prevent MDaemon accounts connecting from reserved IPs from sending more than the specified number of messages in the designated number of minutes. Reserved IP addresses are mostly as defined by RFCs (for example, 127.0.0.*, 192.168.*.*, 10.*.*.*, 172.16.0.0/12, ::1, FD00::/8, FEC0::/10, and FE80::/64).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Limit messages sent from local IPs to [xx] msgs in [xx] minutes
Use this option to prevent MDaemon accounts connecting from any local IPs from sending more than the specified number of messages in the designated number of minutes. Local IPs are all IP addresses configured for any of your MDaemon domain.

Limit messages sent from all other IPs to [xx] msgs in [xx] minutes
Use this option to prevent MDaemon accounts connecting from any other IPs from sending more than the specified number of messages in the designated number of minutes.

Freeze accounts when limit is reached
Check this box if you wish to freeze accounts that attempt to send more than the allowable number of messages. When this happens, the server sends a 552 error, the connection is dropped, and the account is immediately frozen. The frozen account will no longer be able send mail or check its mail, but MDaemon will still accept incoming mail for the account. Finally, when the account is frozen an email is then sent to the postmaster about the account. If the postmaster wishes to re-enable the account, he can simply reply to the message.

White List
Use the *White List* to designate any addresses that you wish to exempt from Account Hijack Detection. Wildcards are permitted. For example, "`newsletters@example.com`" would exempt example.com's "newsletters" MDaemon account, while "`*@newsletters.example.com`" would exempt all MDaemon accounts belonging to the newsletters.example.com domain. The Postmaster account is automatically exempt from Account Hijack Detection.

4.5.4 SSL & TLS

MDaemon supports the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol for SMTP, POP, and IMAP, and for WorldClient's web server. The SSL protocol, developed by Netscape Communications Corporation, is the standard method for securing server/client Internet communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connection. Further, because SSL is built into all current major browsers, simply installing a valid digital certificate on your server will activate the connecting browser's SSL capabilities when connecting to WorldClient.

If you are connecting to the standard mail ports via a mail client instead of using WorldClient, MDaemon supports the STARTTLS extension over TLS for SMTP and IMAP, and the STLS extension for POP3. However, you must first have your client configured to use SSL, and it must support those extensions—not all mail clients support them.

Finally, you can also dedicate specific ports for SSL connections. This isn't required but can provide a further level of accessibility for clients that do not support certain SSL extensions. For example, some versions of Microsoft Outlook Express don't support STARTTLS for IMAP over the default mail port, but do support connections to dedicated SSL ports.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

The options for enabling and configuring SSL are located under the SSL & TLS section of the Security Settings dialog at: Security » Security Settings » SSL & TLS. The SSL port settings for SMTP, POP3, and IMAP are located on the Ports 56 screen at: Setup » Server Settings.

For information on creating and using SSL Certificates, see:

Creating & Using SSL Certificates 500

—

The TLS/SSL protocol is addressed in RFC-2246, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2246.txt

The STARTTLS extension for SMTP is addressed in RFC-3207, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc3207.txt

Using TLS with the IMAP and POP3 protocols is addressed in RFC-2595, which can be viewed at:

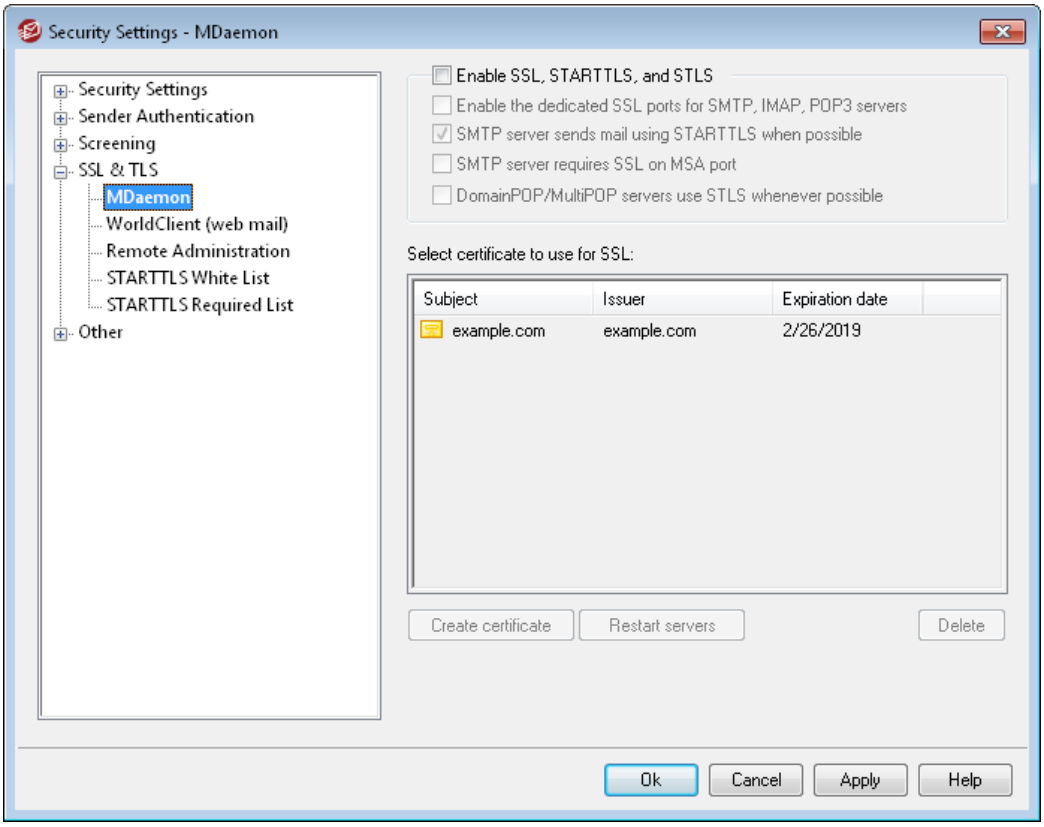
http://www.rfc-editor.org/rfc/rfc2595.txt

See:

SSL & TLS » MDaemon 489
SSL & TLS » WorldClient 492
SSL & TLS » Remote Administration 495

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.4.1 MDaemon



Enable SSL, STARTTLS, and STLS
Click this check box to activate support for the SSL/TLS protocol and the STARTTLS and STLS extensions. Then, choose the certificate that you want to use from the list below.

Enable the dedicated SSL ports for SMTP, IMAP, POP3 servers
Click this option if you want to make available the dedicated SSL ports specified on Ports 56 under Default Domains & Servers. This will not affect clients using STARTTLS and STLS on the default mail ports — it merely provides an additional level of support for SSL.

SMTP server sends mail using STARTTLS when possible
Click this option if you want MDaemon to attempt to use the STARTTLS extension for every SMTP message it sends. If a server to which MDaemon is connecting doesn't support STARTTLS then the message will be delivered normally without using SSL. Use the White List 499 in this section if you wish to prevent the use of STARTTLS for certain domains.

SMTP server requires SSL on MSA port
Enable this option if you wish to require SSL for connections to the server made on the MSA port 56.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

DomainPOP/MultiPOP servers use STLS whenever possible
Check this box if you want the DomainPOP and MultiPOP servers to use the STLS extension whenever possible.

Select certificate to use for HTTPS/SSL

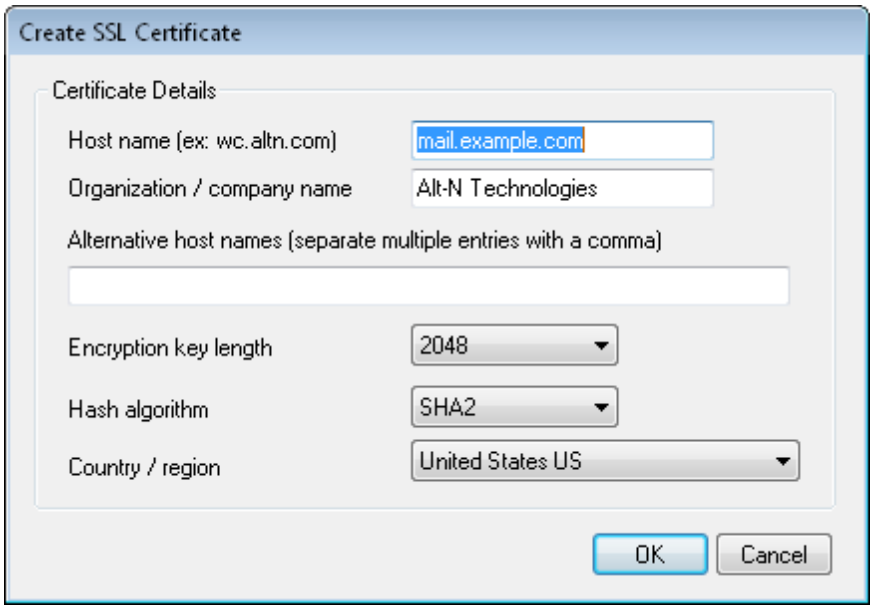
This box displays your SSL certificates. Click a certificate to designate it as the one MDaemon will use. Double-click a certificate to open it in the Certificate dialog for review.

> MDaemon does not support different certificates for multiple domains. All mail domains must share a single certificate. If you have more than one domain then enter those domain names under the option, *Alternative host names (separate multiple entries with a comma)* outlined below.

Delete
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Host name
When creating a certificate, enter the host name to which your users will connect (for example, "mail.example.com").

Organization/company name
Enter the organization or company that "owns" the certificate here.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Alternative host names (separate multiple entries with a comma)
MDaemon does not support separate certificates for multiple domains — all domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, then enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Country/region
Choose the country or region in which your server resides.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Restart servers

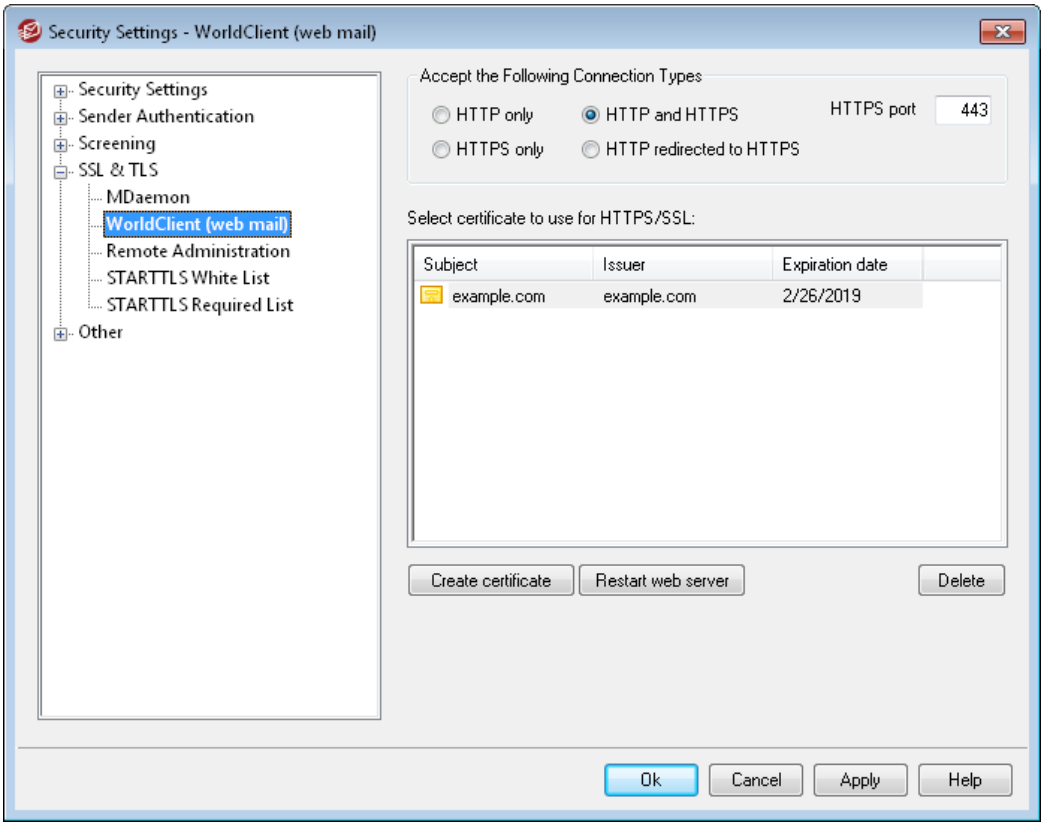
Click to restart the SMTP/IMAP/POP servers. The servers must be restarted when a certificate changes.

See:

SSL & TLS 487
Creating and Using SSL Certificates 500

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.4.2 WorldClient



MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. SSL is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring WorldClient to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » WorldClient (web mail)". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » WorldClient".

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 487

This screen only applies to WorldClient when using MDaemon's built-in web server. If you configure WorldClient to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

Accept the Following Connection Types

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

HTTP only
Choose this option if you do not wish to allow any HTTPS connections to WorldClient. Only HTTP connections will be accepted.

HTTP and HTTPS
Choose this option if you want to enable SSL support within WorldClient, but do not wish to force your WorldClient users to use HTTPS. WorldClient will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the WorldClient TCP port designated on the Web Server 229 screen of WorldClient (web mail).

HTTPS only
Choose this option if you wish to require HTTPS when connecting to WorldClient. WorldClient will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

HTTP redirected to HTTPS
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

HTTPS port
This is the TCP port that WorldClient will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in WorldClient's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the WorldClient port that is designated on the Web Server 229 screen of WorldClient (web mail). If you are still allowing HTTP connections to WorldClient then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

Select certificate to use for HTTPS/SSL

This box displays your SSL certificates. Click a certificate to designate it as the one WorldClient will use. Double-click a certificate to open it in the Certificate dialog for review.

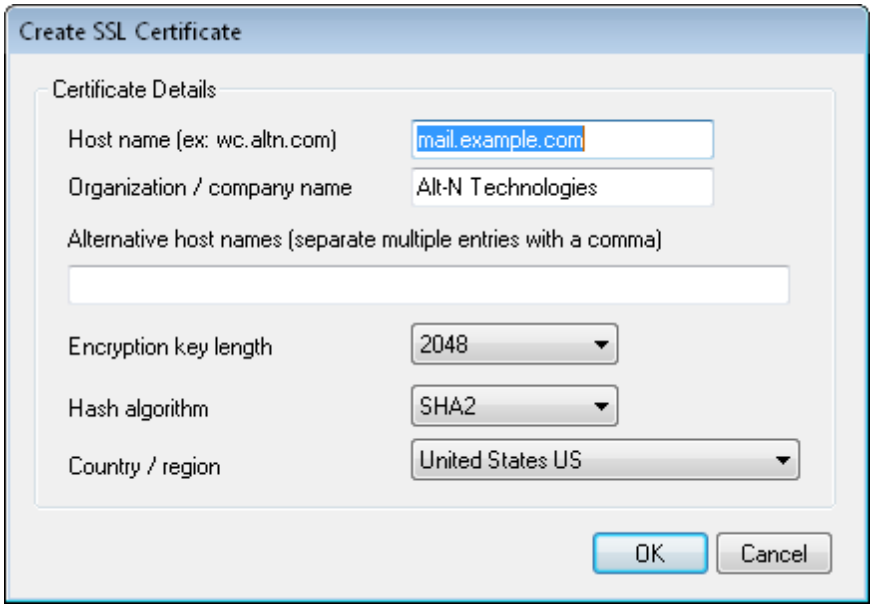
MDaemon does not support multiple certificates for WorldClient. All WorldClient domains must share a single certificate. If you have more than one WorldClient domain then enter those domain names (and any others that you wish to use to access WorldClient) into the option called "*Alternative host names (separate multiple entries with a comma)*" outlined below.

Delete
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Host name
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

Organization/company name
Enter the organization or company that "owns" the certificate here.

Alternative host names (separate multiple entries with a comma)
MDaemon does not support multiple certificates — all WorldClient domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Country/region
Choose the country or region in which your server resides.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

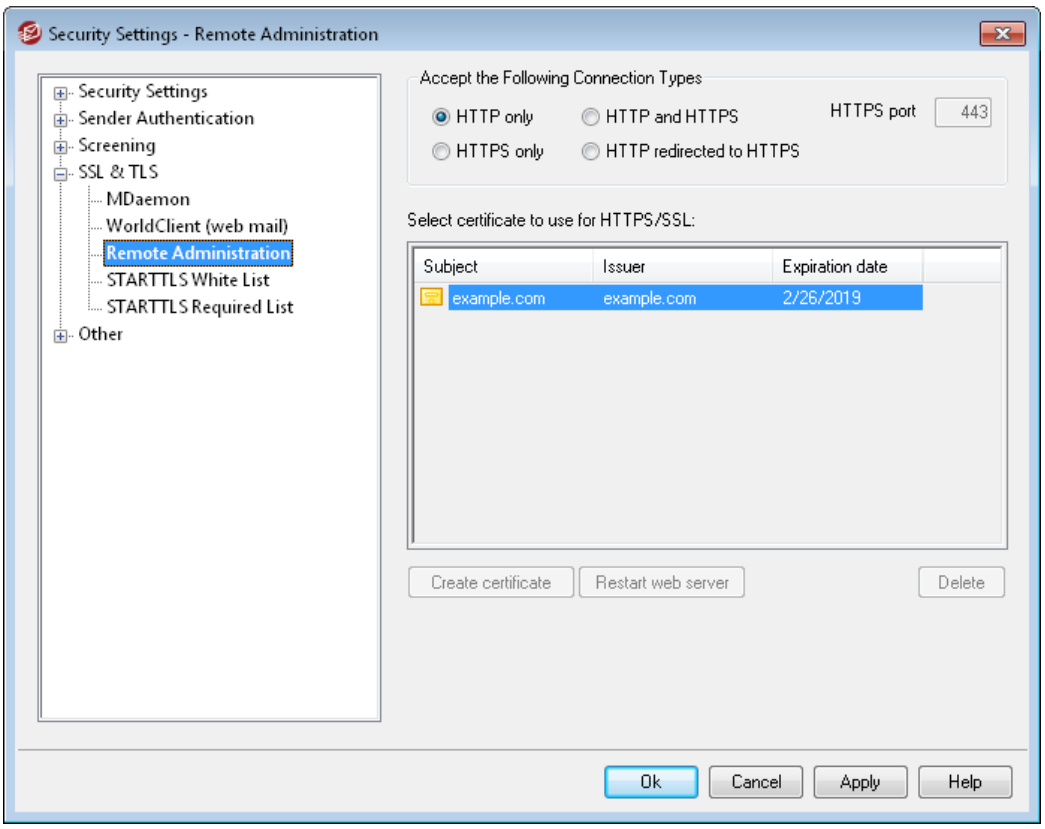
Restart web server

Click this button to restart the web server. The web server must be restarted before a new certificate will be used.

See:

SSL & Certificates 487
Creating and Using SSL Certificates 500

4.5.4.3 Remote Administration



MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. SSL is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring Remote Administration to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » Remote Administration". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » Remote Administration".

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 487

This screen only applies to Remote Administration when using MDaemon's built-in web server. If you configure Remote Administration to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

Accept the Following Connection Types

HTTP only
Choose this option if you do not wish to allow any HTTPS connections to Remote Administration. Only HTTP connections will be accepted.

HTTP and HTTPS
Choose this option if you want to enable SSL support within Remote Administration, but do not wish to force your Remote Administration users to use HTTPS. Remote Administration will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the Remote Administration TCP port designated on the Web Server 252 screen.

HTTPS only
Choose this option if you wish to require HTTPS when connecting to Remote Administration. Remote Administration will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

HTTP redirected to HTTPS
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

HTTPS port
This is the TCP port that Remote Administration will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in Remote Administration's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the Remote Administration port that is designated on the Web Server 252 screen. If you are still allowing HTTP connections to Remote Administration then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

Select certificate to use for HTTPS/SSL

This box displays your SSL certificates. Click a certificate to designate it as the one Remote Administration will use. Double-click a certificate to open it in the Certificate dialog for review.

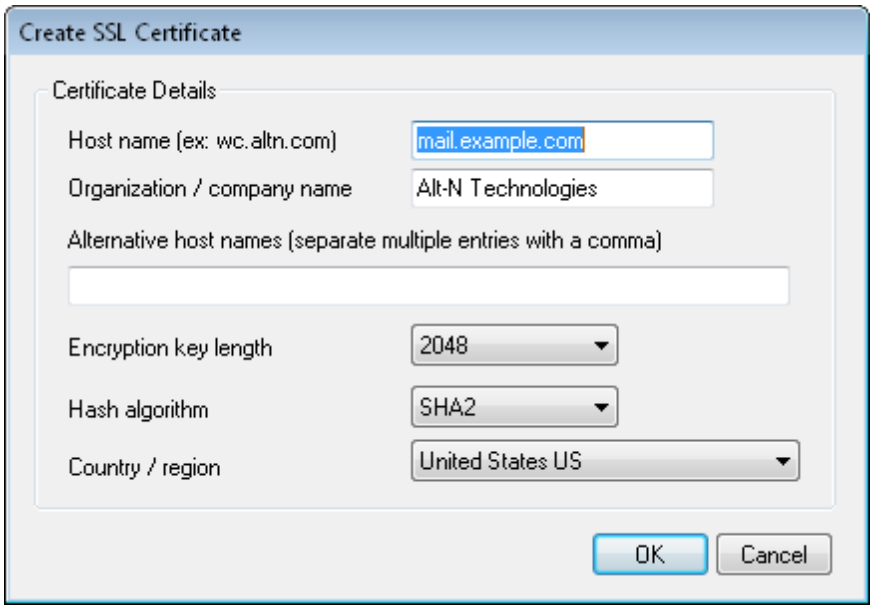
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

MDaemon does not support multiple certificates for Remote Administration. All domains must share a single certificate. If you have more than one domain then enter those domain names (and any others that you wish to use to access Remote Administration) into the option called "*Alternative host names (separate multiple entries with a comma)*" outlined below.

Delete
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Host name
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

Organization/company name
Enter the organization or company that "owns" the certificate here.

Alternative host names (separate multiple entries with a comma)
MDaemon does not support multiple certificates — all Remote Administration domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Country/region
Choose the country or region in which your server resides.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Restart web server

Click this button to restart the web server. The web server must be restarted before a new certificate will be used.

For more information on SSL and Certificates, see:

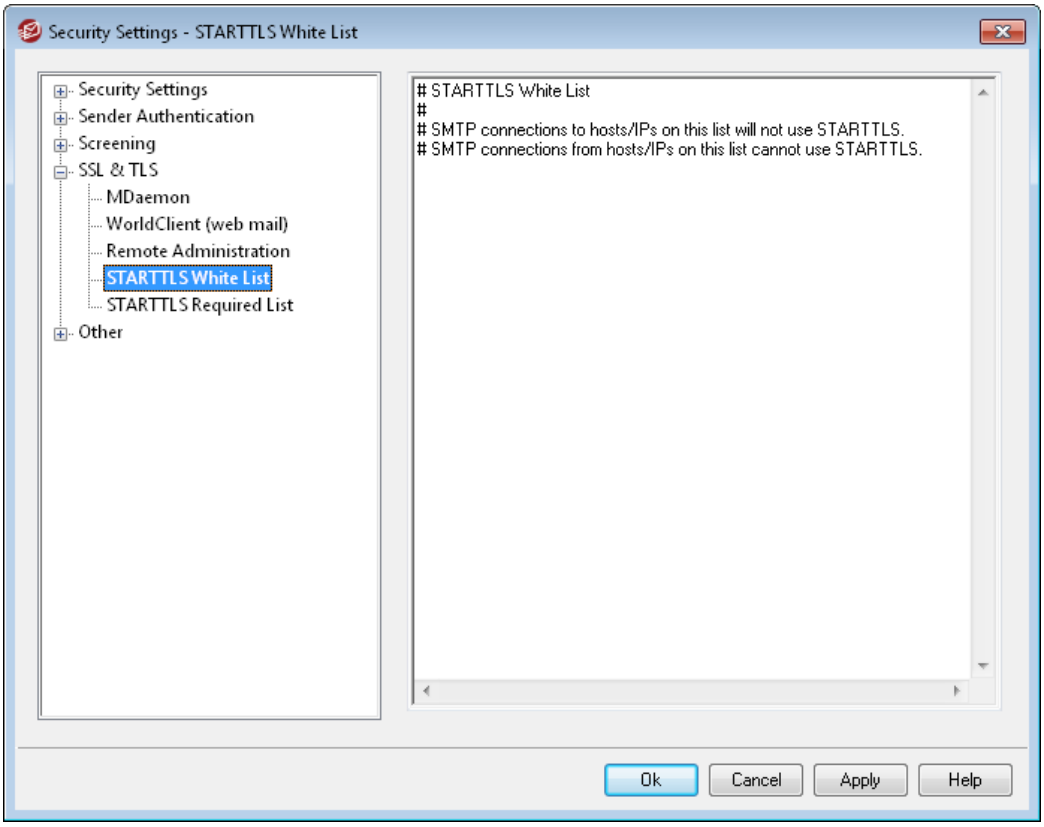
Running Remote Administration under IIS 258
SSL and Certificates 487
Creating and Using SSL Certificates 500

For more information on Remote Administration, see:

Remote Configuration 251
Remote Administration » Web Server 252
Web Access Defaults 587
Account Editor » Web 526

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.4.4 STARTTLS White List



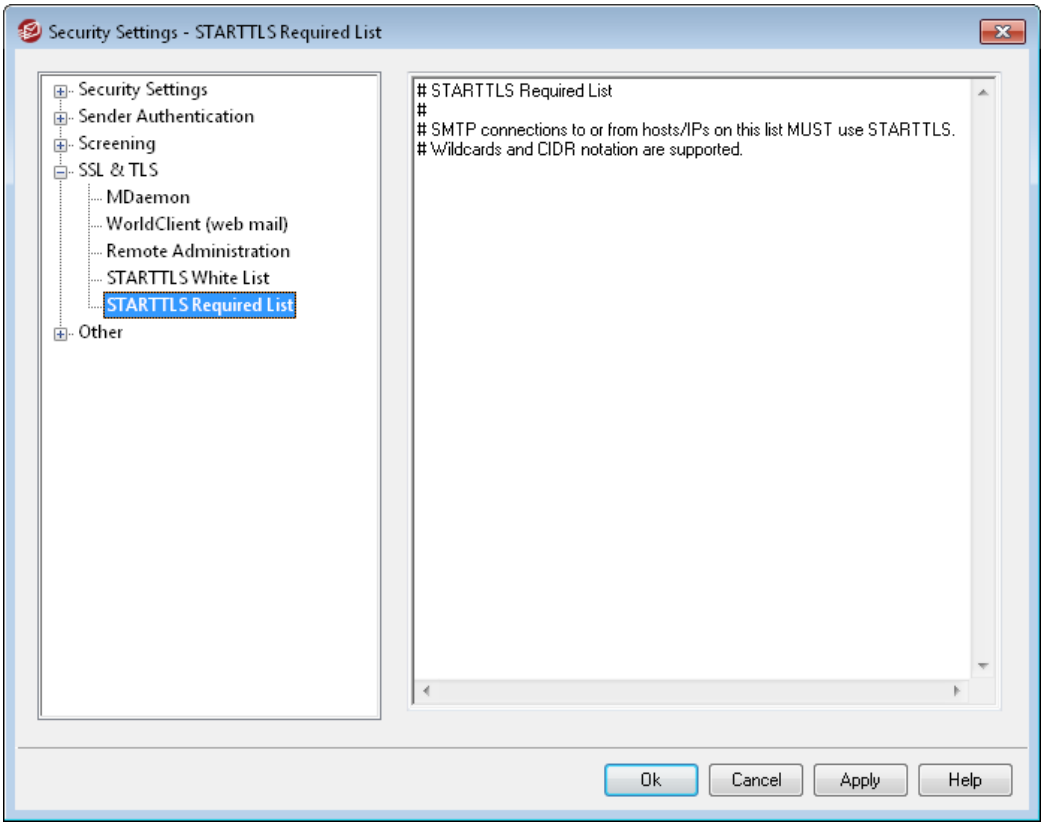
Use this white list to prevent the use of STARTTLS when sending or receiving mail to or from certain hosts or IP addresses.

The STARTTLS extension for SMTP is addressed in RFC-3207, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc3207.txt

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.4.5 STARTTLS Required List



Use this screen to specify hosts and IP addresses that require the use of the STARTTLS extension in order to send or receive mail to or from your server.

The STARTTLS extension for SMTP is addressed in RFC-3207, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc3207.txt

4.5.4.6 Creating and Using SSL Certificates

When using the SSL & TLS dialog to create certificates, MDaemon generates certificates that are self-signed. In other words, the issuer of the certificate, or Certificate Authority (CA), is the same as the owner of the certificate. This is perfectly valid and allowed, but because the CA won't already be listed in yours users' lists of trusted CAs, whenever they connect to WorldClient or Remote Administration's HTTPS URL they will be asked whether or not they wish to proceed to the site and/or install the certificate. Once they agree to install the certificate and trust your WorldClient's domain as a valid CA they will no longer have to see the security alert message when connecting to WorldClient or Remote Administration.

When connecting to MDaemon via a mail client such as Microsoft Outlook, however, they will not be given the option to install the certificate. They will be allowed to choose whether or not they wish to continue using the certificate temporarily, even

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

though it isn't validated. Each time they start their mail client and connect to the server, they will have to choose to continue using the non-validated certificate. To avoid this you should export your certificate and distribute it to your users via email or some other means. Then, they can manually install and trust your certificate to avoid future warning messages.

Creating a Certificate

To create a certificate from within MDaemon:

1. Move to the SSL & TLS dialog within MDaemon (click Security » Security Settings » SSL & TLS » MDaemon).
2. Check the box labeled, "*Enable SSL, STARTTLS, and STLS*".
3. In the text box labeled, "*Host name*", enter the domain to which the certificate belongs (for example, "mail.example.com").
4. Type the name of the organization or company that owns the certificate into the text box labeled, "*Organization/company name*".
5. In "*Alternative host names...*", type all other domain names that your users will be using to access your server (for example, "*.example.com", "example.com", "mail.altn.com", and so on).
6. Choose a length for the encryption key from the drop-down list box.
7. Choose the Country/region where your server resides.
8. Click **Create certificate**.

Using Certificates Issued by a Third-party CA

If you have purchased or otherwise generated a certificate from some source other than MDaemon, you can still use that certificate by using the Microsoft Management Console to import it into the certificate store that MDaemon uses. To do so in Windows XP:

1. On your Windows toolbar, click **Start » Run...** and then type "**mmc /a**" into the text box.
2. Click **OK**.
3. In the Microsoft Management Console, click **File » Add/Remove Snap-in...** on the menu bar (or press **Ctrl+M** on your keyboard).
4. On the Standalone tab, click **Add...**
5. On the *Add Standalone Snap-in* dialog, click **Certificates**, and then click **Add**.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

6. On the *Certificates snap-in* dialog, choose **Computer account**, and then click **Next**.
7. On the *Select Computer* dialog, choose **Local computer**, and then click **Finish**.
8. Click **Close**, and click **OK**.
9. Under *Certificates (Local Computer)* in the left pane, if the certificate that you are importing is self-signed, click **Trusted Root Certification Authorities** and then **Certificates**. If it is not self-signed then click **Personal**.
10. On the menu bar, click **Action** » **All Tasks** » **Import...**, and click **Next**.
11. Enter the file path to the certificate that you wish to import (using the Browse button if necessary), and click **Next**.
12. Click **Next**, and click **Finish**.

MDaemon will only display certificates that have private keys using the Personal Information Exchange format (PKCS #12). If your imported certificate does not appear in the list then you may need to import a `*.PEM` file, which contains both a certificate key and private key. Importing this file using the same process outlined above will convert it to the PKCS #12 format.

See:

SSL & TLS 487

4.5.5 Other

4.5.5.1 Backscatter Protection - Overview

Backscatter

"Backscatter" refers to response messages that your users receive to emails that they never sent. This occurs when spam messages or messages sent by viruses contain a "Return-Path" address that is forged. Consequently, when one of these messages is rejected by the recipient's server, or if the recipient has an Autoresponder or "out of office"/vacation message associated with his account, the response message will then be directed to the forged address. This can lead to huge numbers of bogus Delivery Status Notifications (DSNs) or auto response messages ending up in your users' mailboxes. Further, spammers and virus authors frequently take advantage of this phenomenon and will sometimes use it to launch Denial of Service (DoS) attacks against email servers, causing a flood of invalid emails to arrive from servers located all over the world.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

MDaemon's Solution

To combat backscatter, MDaemon contains a feature called Backscatter Protection (BP). BP can help to ensure that only legitimate Delivery Status Notifications and Autoresponders get delivered to your accounts, by using a private key hashing method to generate and insert a special time-sensitive code into the "Return-Path" address of your users' outgoing messages. Then, when one of these messages encounters a delivery problem and is bounced back, or when an auto-reply is received with a "mailer-daemon@..." or NULL reverse path, MDaemon will see the special code and know that it is a genuine automated reply to a message that was sent by one of your accounts. If the address doesn't contain the special code, or if the code is more than seven days old, it will be logged by MDaemon and can be rejected.

Backscatter Protection 504 is located under MDaemon's Security menu at: Security » Security Settings » Other » Backscatter Protection.

Backscatter Protection is an implementation of Bounce Address Tag Validation (BATV). For more on BATV, visit:

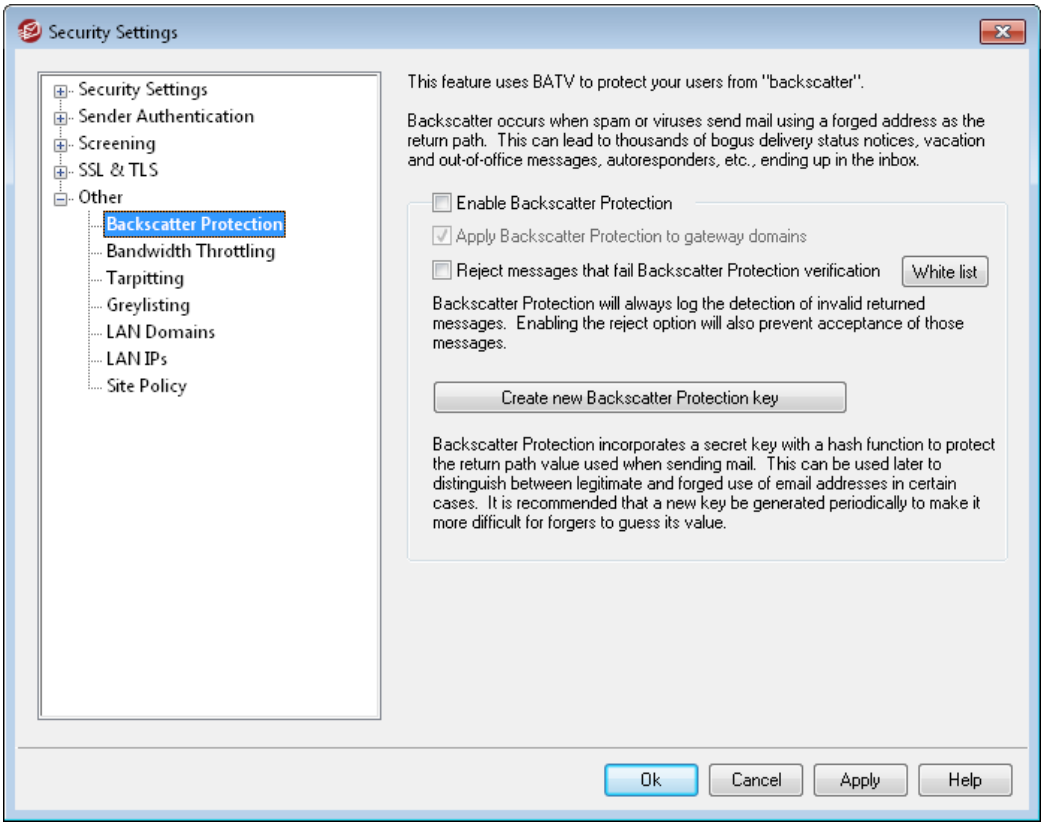
http://www.mipassoc.org/batv/

See:

Backscatter Protection 504

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.5.1.1 Backscatter Protection


Security Settings
Security Settings
Sender Authentication
Screening
SSL & TLS
Other
Backscatter Protection
Bandwidth Throttling
Tarpitting
Greylisting
LAN Domains
LAN IPs
Site Policy
This feature uses BATV to protect your users from "backscatter".
Backscatter occurs when spam or viruses send mail using a forged address as the return path. This can lead to thousands of bogus delivery status notices, vacation and out-of-office messages, autoresponders, etc., ending up in the inbox.
Enable Backscatter Protection
Apply Backscatter Protection to gateway domains
Reject messages that fail Backscatter Protection verification
White list
Backscatter Protection will always log the detection of invalid returned messages. Enabling the reject option will also prevent acceptance of those messages.
Create new Backscatter Protection key
Backscatter Protection incorporates a secret key with a hash function to protect the return path value used when sending mail. This can be used later to distinguish between legitimate and forged use of email addresses in certain cases. It is recommended that a new key be generated periodically to make it more difficult for forgers to guess its value.
Ok
Cancel
Apply
Help

Backscatter Protection

Enable Backscatter Protection
Click this checkbox if you wish to insert a special Backscatter Protection code into each outgoing message's "Return-Path" address. MDaemon will generate this special code by using the private key found in the `rsa.private` file located in MDaemon's `PEM\_batv\` folder, and the code will be valid for seven days. Any incoming DSNs or other auto-response messages (with a "`mailer-daemon@...`" or `NULL` reverse path) must have a valid, non-expired BP code or they will fail BP verification.

If you disable this option, MDaemon will not insert the special Backscatter Protection code into outgoing messages. It will, however, continue to check incoming DSNs and auto-response messages to ensure that any incoming message with a valid code is not rejected by mistake.

Apply Backscatter Protection to gateway domains
When Backscatter Protection is enabled, click this option if you also wish to apply it to domains for which MDaemon is acting as a gateway or backup server (see Gateway Manager 162).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Reject messages that fail Backscatter Protection verification
Click this checkbox if you wish to reject DSNs or other auto-response messages that fail BP verification. Messages with a "mailer-daemon@..." or NULL reverse path will fail if they do not contain the special code or if the code's seven day life-cycle has expired. Because of Backscatter Protection's solid reliability, there are no false positives or "gray areas" — a message is valid or it isn't. For this reason it is safe to configure MDaemon to reject invalid messages, as long as you ensure that all of your accounts' outgoing messages contain the special BP code. In all cases, however, the result of BP verification will be logged into the SMTP-in log file, even when you choose not to reject messages that fail verification. Incoming messages for gateways will not be rejected unless you have checked the *...apply Backscatter Protection to gateway domains* option above.

When you enable Backscatter Protection, you should wait about a week before setting it to reject invalid auto-response messages. This is because during that time you might still receive DSNs or auto-responses to messages that were sent out before BP was activated. If BP were configured to reject invalid message during that time then those legitimate response messages would be rejected by mistake. After a week it should be safe to start rejecting invalid messages. This same warning applies when you create a new BP key and choose to delete the old key immediately instead of allowing it to continue working for another seven days. (see the *Create new Backscatter Protection key* option below).

White List
Click this button to open the Backscatter Protection white list. Use this list to designate any IP addresses or domains that you wish to exempt from Backscatter Protection.

Create new Backscatter Protection key
Click this button to generate a new Backscatter Protection key. This key is used by MDaemon to create and then verify the special BP codes that are inserted into messages. The key is located in a file called rsa.private in MDaemon's PEM_batv\ folder. When the new key is generated, a box will open to inform you that the old key will continue to work for seven more days unless you wish to delete it immediately. In most cases you should click "**No**", electing to allow the key to work for seven more days. If you choose to delete the key immediately then that could cause some incoming messages to fail BP verification, since they would be responses to messages containing the special code generated by the old key.

If you have your email traffic split across multiple servers, you may need to share the key file with all of your other servers or Mail Transfer Agents (MTAs).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Backscatter Protection - Overview 502

4.5.5.2 Bandwidth Throttling - Overview

The Bandwidth Throttling feature makes it possible for you to police the consumption of bandwidth used by MDaemon. You can control the rate at which sessions or services progress — you can set different rates for each of MDaemon's major services on a per-domain basis, including the Domains and Domain Gateways. You can also set limits on local connections by selecting "Local traffic" from a drop down box. This will allow you to create special bandwidth settings that will take effect if the connection is either from or to a local IP address or domain name.

Bandwidth Throttling can be applied on either a per-session or per-service basis. When using the per-session mode, each session will be independently throttled to the associated rate. Thus multiple sessions of the same service type occurring simultaneously could exceed a service's configured value. When configured to throttle bandwidth on a per-service basis, MDaemon will monitor the combined use of all sessions of the same service type and allocate equal fractions of the total bandwidth to each. Multiple sessions will then share the configured maximum bandwidth equally. This will allow you to set a limit on an entire service.

When extending Bandwidth Throttling to a Domain Gateway, it must be handled a bit differently than a normal domain since a Domain Gateway doesn't have a specific IP address associated with it. MDaemon must use the value passed in the RCPT command to determine whether or not an inbound SMTP session is bound for the gateway. If it is, then inbound SMTP bandwidth throttling will be applied. Due to the limitations of SMTP, if even one recipient of a multiple recipient message is destined for a Domain Gateway then the entire session will be throttled.

The Bandwidth Throttling system is calibrated in kilobytes per second (KB/s). A value of "0" means that no limit will be applied to the speed at which a session (or service) progresses, thus it will use the maximum amount of available bandwidth. A value of "10", for example, will force MDaemon to deliberately throttle back on the speed of transmission so as to remain at or slightly above 10 KB/s.

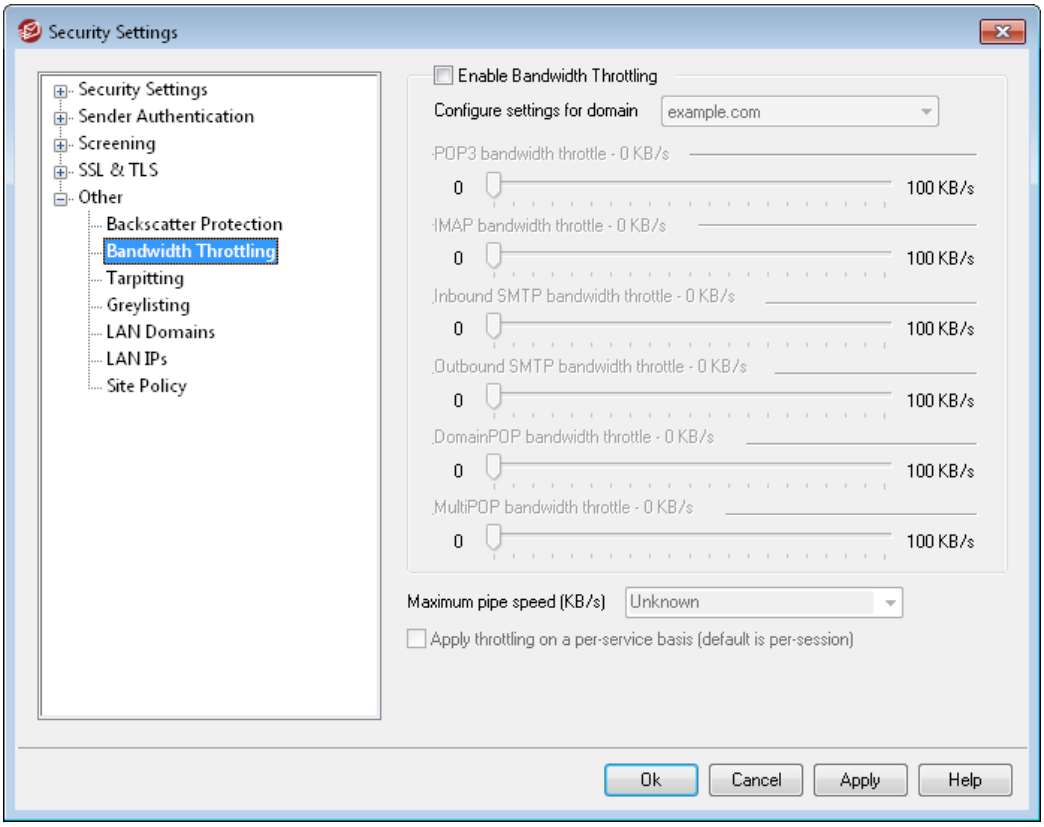
Bursts of activity at the beginning of a session can and will exceed the fixed limits. Throttling takes place and becomes more defined as the session progresses.

See:

Bandwidth Throttling 507
LAN IPs 514

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

4.5.5.2.1 Bandwidth Throttling



Enable Bandwidth Throttling
Check this box if you wish to activate the Bandwidth Throttling feature.

Configure settings for domain
Choose a domain from the drop-down list box and then adjust the options corresponding to the various services to configure bandwidth throttling for the selected domain. A setting of "0" in any particular control means no bandwidth limit is set for that service type. In the drop-down list box, the bottom entry listed is *Local traffic*. Setting bandwidth throttling for this option will determine the limits placed on local traffic (i.e. sessions and services occurring on your local LAN rather than externally). The LAN IPs 514 screen can be used for listing IP addresses that should be treated as local.

Services

[Service type] bandwidth throttle – XX KB/s
After selecting a domain from the drop-down list box, adjust these controls to set bandwidth limitations for the selected domain. A setting of "0" means no bandwidth limit is applied to that particular service type. Setting a slider to any number other than "0" will limit the maximum bandwidth to that number of Kilobytes per second for the designated service.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

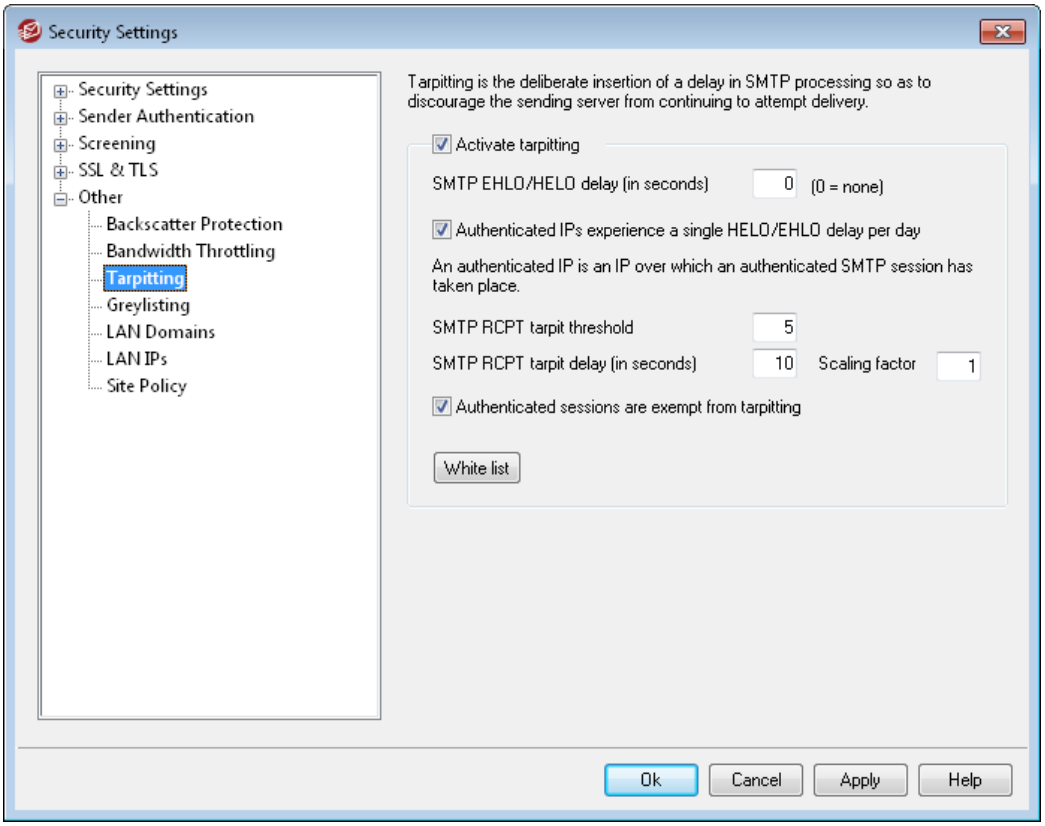
Maximum pipe speed (KB/s)
From the drop-down list box, choose the maximum speed of your connection in Kilobytes per second.

Apply throttling on a per-service basis (default is per-session)
Click this checkbox if you want to throttle bandwidth on a per-service basis rather than the default per-session basis. When throttling on a per-service basis, the service's designated amount of bandwidth will be divided equally among all active sessions of the given service type. Thus, the total amount of bandwidth used, for example, by multiple IMAP clients connecting at the same time could never exceed the designated amount regardless of how many clients were connected. If throttling on a per-*session* basis, then no single IMAP session could exceed the designated limit but the total of multiple simultaneous sessions could.

See:

Bandwidth Throttling - Overview 506

4.5.5.3 Tarpitting


Security Settings
Security Settings
Sender Authentication
Screening
SSL & TLS
Other
Backscatter Protection
Bandwidth Throttling
Tarpitting
Greylisting
LAN Domains
LAN IPs
Site Policy
Tarpitting is the deliberate insertion of a delay in SMTP processing so as to discourage the sending server from continuing to attempt delivery.
Activate tarpitting
SMTP EHLO/HELO delay (in seconds) 0 (0 = none)
Authenticated IPs experience a single HELO/EHLO delay per day
An authenticated IP is an IP over which an authenticated SMTP session has taken place.
SMTP RCPT tarpit threshold 5
SMTP RCPT tarpit delay (in seconds) 10 Scaling factor 1
Authenticated sessions are exempt from tarpitting
White list
Ok
Cancel
Apply
Help

Tarpitting is located under the Security menu at: Security » Security Settings » Other » Tarpitting.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Tarpitting makes it possible for you to deliberately slow down a connection once a specified number of RCPT commands have been received from a message's sender. This is to discourage spammers from trying to use your server to send unsolicited bulk email ("spam"). You can specify the number of RCPT commands allowed before tarpitting begins and the number of seconds to delay the connection each time a subsequent command is received from that host during the connection. The assumption behind this technique is that if takes spammers an inordinately long period of time to send each message then that will discourage them from trying to use your server to do so again in the future.

Activate tarpitting
Click this check box to activate MDaemon's tarpitting features.

SMTP EHLO/HELO delay (in seconds)
Use this option to delay the server response to EHLO/HELO SMTP commands. Delaying the responses by even as little as ten seconds can potentially save a significant amount of processing time by reducing the amount of spam received. Frequently spammers depend on rapid delivery of their messages and therefore do not wait long for a response to EHLO/HELO commands. With even a small delay, spam tools will sometimes give up and move on rather than wait for a response. Connections on the MSA port (designated on the Ports 56 screen under Server Settings) are always exempt from this delay. The default setting for this option is "0", meaning EHLO/HELO will not be delayed.

Authenticated IPs experience a single EHLO/HELO delay per day
Click this check box if you wish to limit the EHLO/HELO delay to once per day for authenticated connections from a given IP address. The first message from that IP address will be delayed, but any subsequent messages sent from the same IP address will not.

SMTP RCPT tarpit threshold
Specify the number of SMTP RCPT commands that you wish to allow for a given host during a mail session before MDaemon will begin tarpitting that host. For example, if this number was set to 10 and a sending host attempted to send a message to 20 addresses (i.e. 20 RCPT commands), then MDaemon would allow the first 10 normally and then pause after each subsequent command for the number of seconds specified in the *SMTP RCPT tarpit delay* control below.

SMTP RCPT tarpit delay (in seconds)
Once the *SMTP RCPT tarpit threshold* is reached for a host, this is the number of seconds that MDaemon will pause after each subsequent RCPT command is received from that host during the mail session.

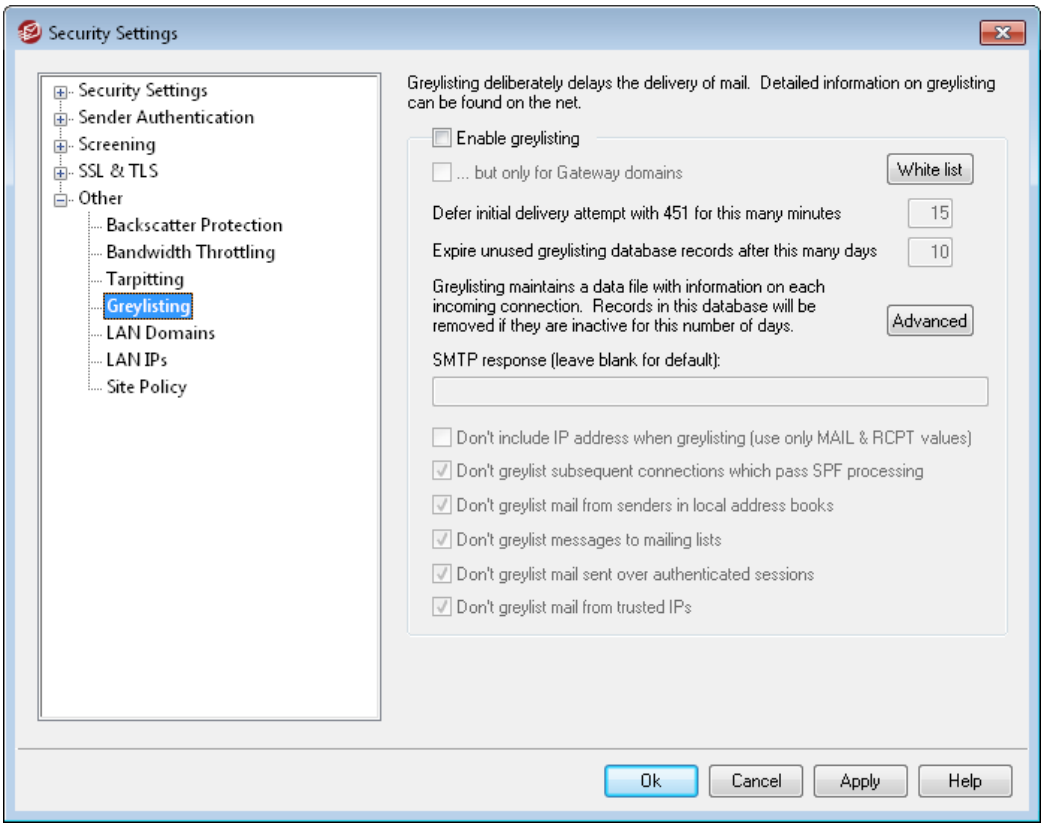
Scaling factor
This value is a multiplier by which the base tarpit delay will be increased over time. When the tarpit threshold is reached and the tarpit delay is applied to a session, each delay will be multiplied by this value to determine to length of the next delay in the session. For example, if the tarpit delay is set to 10 and the scaling factor is set to 1.5 then the first delay will be 10 seconds, the second will be 15 seconds, the third 22.5, then 33.75, and so on (i.e. 10 x 1.5 = 15, 15 x 1.5 = 22.5, etc.). The default Scaling factor is 1, meaning that the delay will not be increased.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Authenticated sessions are exempt from tarpitting
Click this checkbox if you want senders who authenticate their mail session to be exempt from Tarpitting.

White list
Click this button to open the Tarpitting white list. On it you can designate IP addresses that you wish to be exempt from tarpitting.

4.5.5.4 Greylisting


Security Settings
Security Settings
Sender Authentication
Screening
SSL & TLS
Other
Backscatter Protection
Bandwidth Throttling
Tarpitting
Greylisting
LAN Domains
LAN IPs
Site Policy
Greylisting deliberately delays the delivery of mail. Detailed information on greylisting can be found on the net.
Enable greylisting
... but only for Gateway domains
White list
Defer initial delivery attempt with 451 for this many minutes
15
Expire unused greylisting database records after this many days
10
Greylisting maintains a data file with information on each incoming connection. Records in this database will be removed if they are inactive for this number of days.
Advanced
SMTP response (leave blank for default):
Don't include IP address when greylisting (use only MAIL & RCPT values)
Don't greylist subsequent connections which pass SPF processing
Don't greylist mail from senders in local address books
Don't greylist messages to mailing lists
Don't greylist mail sent over authenticated sessions
Don't greylist mail from trusted IPs
Ok
Cancel
Apply
Help

Greylisting is located under the Security dialog at: Security » Security Settings » Other » Greylisting. Greylisting is a spam-fighting technique that exploits the fact that SMTP servers retry delivery of any message that receives a temporary (i.e. "try again later") error code. Using this technique, when a message arrives from a non-white listed or otherwise previously unknown sender, its sender, recipient, and sending server's IP address will be logged and then the message will be refused by Greylisting during the SMTP session with a temporary error code. Furthermore, for a designated period of time (say, 15 minutes) any future delivery attempts will also be temporarily refused. Because "spammers" do not typically make further delivery attempts when a message is refused, greylisting can significantly help to reduce the amount of spam your users receive. But, even if the spammers should attempt to retry delivery at a later time, it is possible that by that time the spammers will have been identified and other spam-fighting options (such as DNS Black Lists 425) will successfully block them.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

It's important to note, however, that this technique can deliberately delay "good" email along with the "bad". But, the legitimate messages should still be delivered sometime later after the greylisting period has expired. It is also important to note that you have no way of knowing how long the sending servers will wait before making further delivery attempts. It is possible that purposely refusing a message with a temporary error code could cause it to be delayed by as little as just a few minutes or by as much as an entire day.

There are several traditional problems and negative side-effects associated with greylisting, and the Greylisting screen contains a number of options designed to deal with them.

First, some sending domains use a pool of mail servers to send outbound mail. Since a different mail server could be used for each delivery attempt, each attempt would be treated as a new connection to the greylisting engine. This could multiply the length of time it would take to get past Greylisting because each of those attempts would be greylisted as if they were separate messages instead of retries of a previous message. By utilizing an SPF lookup option, this problem can be solved for sending domains who publish their SPF data. Furthermore, there is an option to ignore the IP of the sending mail server completely. Using this option lowers the efficiency of greylisting, but it does completely solve the server pool problem.

Second, greylisting traditionally entails a large database since each incoming connection must be tracked. MDaemon minimizes the need to track connections by placing the Greylisting feature nearly last in the SMTP processing sequence. This allows all of MDaemon's other options to refuse a message prior to reaching the greylisting stage. As a result, the size of the greylisting data file is greatly reduced, and since it is memory resident there is little practical performance impact.

Finally, several options are available to minimize the impact of greylisting on "good" messages. First, messages sent to mailing lists can be excluded. Next, Greylisting has its own white list file on which you can designate IP addresses, senders, and recipients that you wish to be exempt from greylisting. Finally, Greylisting contains an option for using each account's private address book files as a white list database. So, mail to a user from someone in that user's address book can be excluded from greylisting.

For more information about greylisting in general, visit Even Harris' site at:

http://projects.puremagic.com/greylisting/

Greylisting

Enable greylisting
Click this option to enable the Greylisting feature within MDaemon.

...but only for Gateway domains
Click this check box if you only wish to greylist messages destined for gateway domains.

White list
This button opens the Greylisting white list on which you can designate senders, recipients, and IP addresses that will be exempt from greylisting.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Defer initial delivery attempt with 451 for this many minutes
Designate the number of minutes for which a delivery attempt will be greylisted after the initial attempt. During that period of time, any subsequent delivery attempts by the same server/sender/recipient combination (i.e. "greylisting triplet") will be refused with another temporary error code. After the greylist period has elapsed, no further greylisting delays will be implemented on that triplet unless its Greylisting database record expires.

Expire unused greylisting database records after this many days
After the initial greylisting period has elapsed for a given greylisting triplet, no further messages matching that triplet will be delayed by Greylisting. However, if no message matching that triplet is received for the number of days designated in this option, its Greylisting database record will expire. A subsequent attempt by that triplet will cause a new Greylisting record to be created it will have to go through the initial greylisting period again.

Advanced
Click this button to open the Greylisting database, which you can use to review or edit your greylisting triplets.

SMTP response (leave blank for default)
If you provide a custom string of text in this space then MDaemon will return the SMTP response, "`451 <your custom text>`" rather than the default "`451 Greylisting enabled, try again in X minutes.`" This is useful, for example, if you wish to provide a string that contains a URL to a description of greylisting.

Don't include IP address when greylisting (use only MAIL & RCPT values)
Click this check box if do not wish to use the sending server's IP address as one of the greylisting parameters. This will solve the potential problem that can be caused by server pools, but it will reduce Greylisting's efficiency.

Don't greylist subsequent connections which pass SPF processing
When using this option, if an incoming message matches a triplet's sender and recipient but not the sending server, but SPF processing determines that the sending server is a valid alternate to the one listed in the triplet, then the message will be treated as a subsequent delivery matching that triplet rather than a new connection requiring a new Greylisting record.

Don't greylist mail from senders in local address books
Click this option if you wish to exempt a message from greylisting when its sender is listed in the recipient's address book.

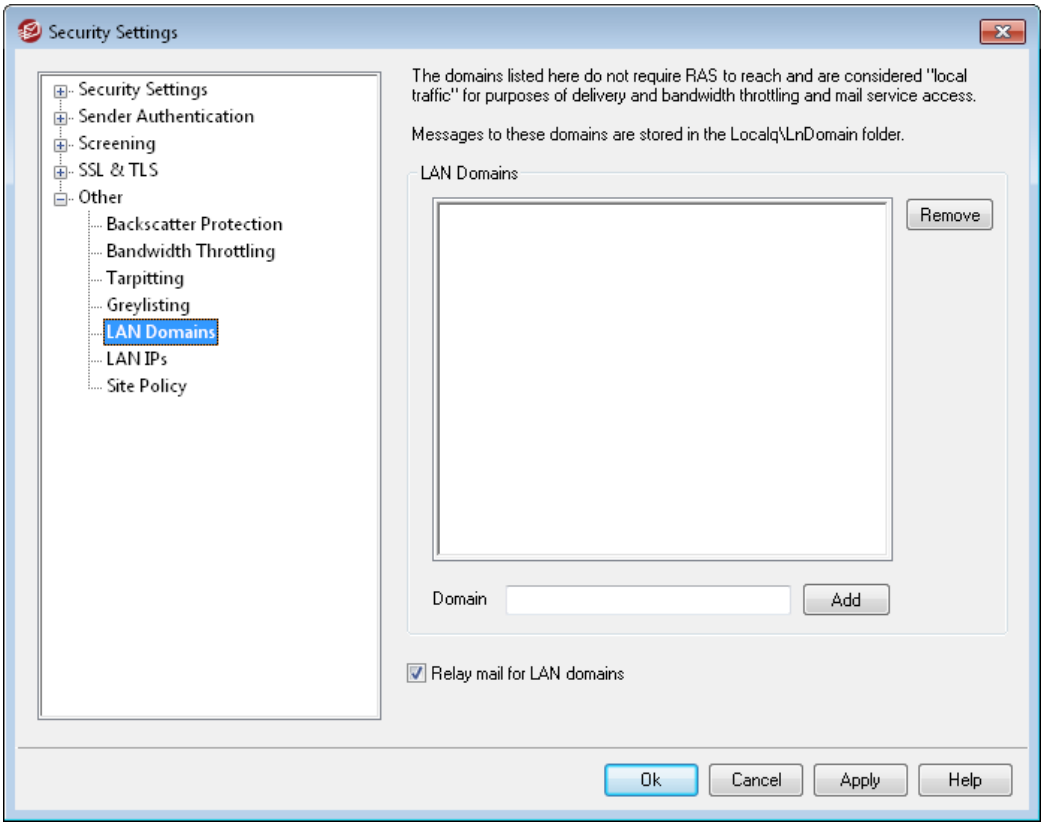
Don't greylist messages to mailing lists
Click this check box if you wish to exempt mailing list messages from greylisting.

Don't greylist mail sent over authenticated sessions
Use this option if you wish all messages coming in over an authenticated session to be exempt from greylisting.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Don't greylist mail from trusted IPs
Use this option if you wish all messages coming from trusted IP addresses to be exempt from greylisting.

4.5.5.5 LAN Domains



LAN Domains

The domains listed here are considered by MDaemon to be part of your local LAN (local area network). Therefore, no dialup or Internet connection is required in order to deliver a message to one of them.

Domain
Enter a domain name and then click *Add* to add it to the list.

Add
After specifying a domain in the *Domain* option above, click this button to add it to the list.

Remove
Select a domain in the list and then click this button to remove it.

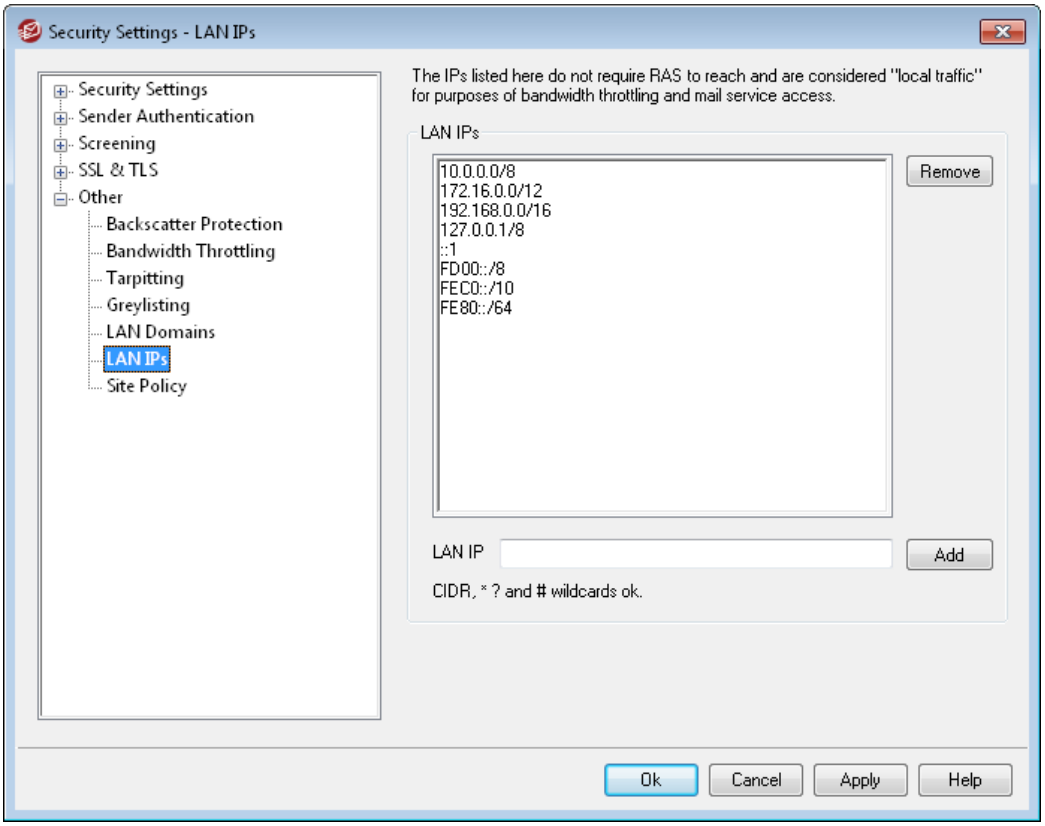
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Relay mail for LAN domains
If this box is checked MDaemon will relay mail for these domains. This provides some measure of control over the traffic sent to and from these domains.

See:

LAN IPs 514

4.5.5.6 LAN IPs



LAN IPs

Similar to LAN Domains 513, this screen is used to list IP addresses that reside on your LAN (local area network). These IP addresses therefore do not require RAS or an Internet connection to reach them, and they are treated as local traffic for the purposes of bandwidth throttling. Further, there are various other security and spam prevention restrictions that they may be exempt from since they are local addresses.

Remove
Select an IP address from the list and then click this button to remove it.

LAN IP
Enter an IP address to add to the LAN IPs list and click *Add*. Wildcards like 127.0.*.*

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

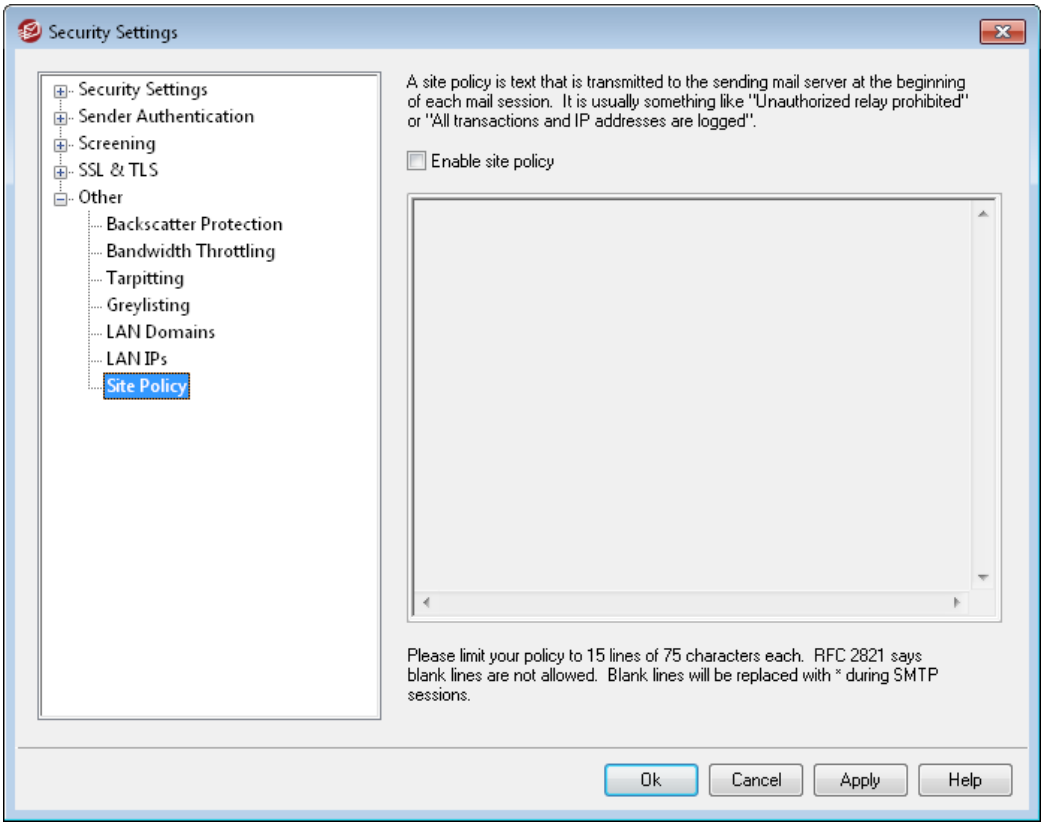
are permitted.

Add
After entering an IP Address into the *LAN IP* control, click this button to add it to the list.

See:

LAN Domains 513

4.5.5.7 Site Policy


Security Settings
Security Settings
Sender Authentication
Screening
SSL & TLS
Other
Backscatter Protection
Bandwidth Throttling
Tarpitting
Greylisting
LAN Domains
LAN IPs
Site Policy
A site policy is text that is transmitted to the sending mail server at the beginning of each mail session. It is usually something like "Unauthorized relay prohibited" or "All transactions and IP addresses are logged".
Enable site policy
Please limit your policy to 15 lines of 75 characters each. RFC 2821 says blank lines are not allowed. Blank lines will be replaced with * during SMTP sessions.
Ok
Cancel
Apply
Help

Creating an SMTP Site Policy Statement
Use this dialog to specify a Site Policy statement for your server. The text is stored in the `policy.dat` file located in MDaemon's `\app\` subfolder and is transmitted to sending servers at the beginning of every SMTP mail session. An example of a common site policy is, "`This server does not relay`" or "`Unauthorized use prohibited`." You do not need to prepend each line with "`220`" or "`220-`". MDaemon handles each line accordingly, either with or without these prepended codes.

A site usage policy with a statement regarding relaying of mail would look like this during the SMTP transaction:

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

```
220-Alt-N Technologies ESMTP MDaemon
220-This site does relay unauthorized email.
220-If you are not an authorized user of our server
220-then you must not relay mail through this site.
220
HELO example.com...
```

The POLICY.DAT file must be comprised of printable ASCII text only and have no more than 512 characters per line; however it is highly recommended that you use no more than 75 characters per line. The maximum size of this file is 5000 bytes. MDaemon will not display files larger than 5000 bytes.

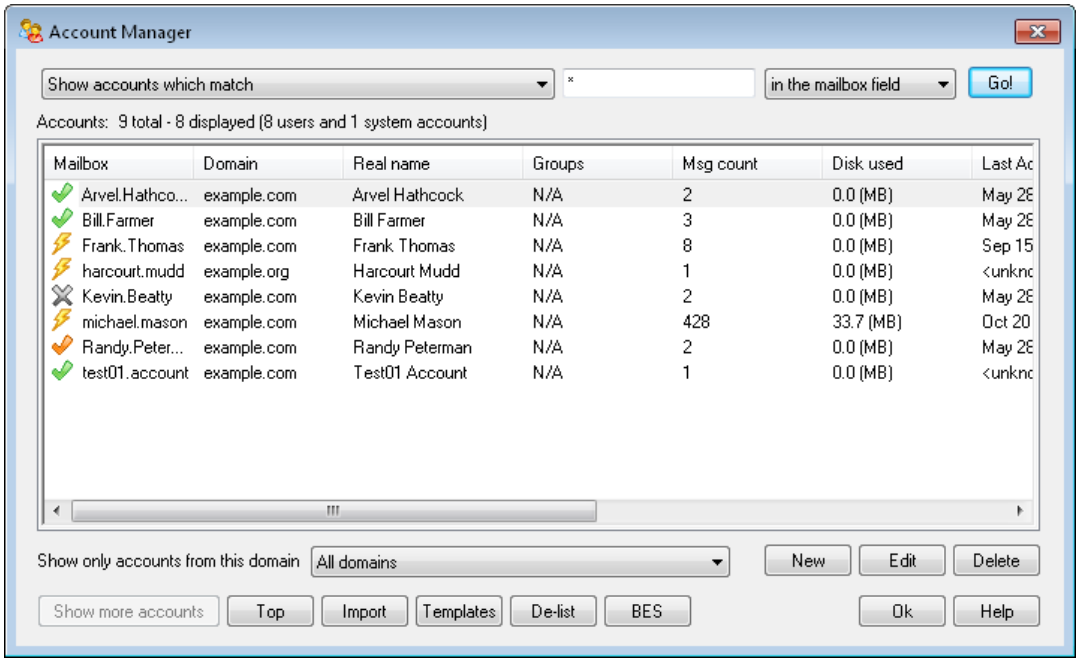
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Section V

5 Accounts Menu

5.1 Account Manager

To better manage the selection, addition, deletion, or modification of your accounts, MDaemon contains the Account Manager. This dialog provides access to account information and can be used to sort accounts by mailbox, domain, real name, or mail folder. The Account Manager is located under the Accounts menu at: Accounts » Account Manager...



Account Management

Above the list of accounts you will see two statistics regarding the list. The first number is the total number of MDaemon user accounts that currently exist on your system. The second number is the number of those accounts currently displayed in the list. The accounts that will be displayed is contingent upon what you have chosen in the *Show only accounts from this domain* option below the list. If you have selected "All Domains" then all of your MDaemon accounts will be displayed in the list. There is a search option at the top of this dialog that you can use to define exactly which accounts will be displayed beyond simply the domain to which they belong.

Each entry in the list contains an Account Status Icon (see below), the mailbox, the domain to which it belongs, the "real name" of the account holder, any groups to which the account belongs, the message count, the disk space used (in MB), the last time the account was accessed, and the mail folder in which the account's messages are stored. This list can be sorted in ascending and descending order by whichever column that you prefer. Click any column heading to sort the list in ascending order by that column. Click the column again to sort it in descending order.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

By default, only 500 accounts at a time will be displayed in this list. If you want to see more accounts from the currently selected domain (or All Domains, if you have selected that option) then you must click the *Show more accounts* button to display the next 500. If you want to be able to display more than 500 accounts at a time then open the `MDaemon.ini` file and change the `MaxAccountManagerEntries=500` key to whatever value that you prefer.

Account Status Icons

Account is a global or domain administrator.

Full access account. Both POP and IMAP access are enabled.

Restricted access account. Either POP, IMAP, or both are disabled.

Account is frozen. MDaemon will still accept mail for the account, but the user cannot send or check mail.

Disabled account. All access to the account is disabled.

New
Click this button to open the Account Editor 521 in order to create a new account.

Edit
Select an account from the list and then click this button to open it in the Account Editor 521. You can also double-click the account to open it.

Delete
Select an account from the list and then click this button to delete it. You will be asked to confirm your decision to delete the account before MDaemon will proceed.

Show only accounts from this domain
Choose "All Domains" from this drop-down list box to display all MDaemon accounts. Choose a specific domain to show only that domain's accounts.

Show more accounts
The account list will only display 500 accounts at a time. If there are more than 500 accounts in the domain that you have chosen then click this button to display the next 500. See the note above for instructions on how to increase the maximum number of accounts that may be displayed.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Top
Click this button to quickly move to the top of the account list.

Import
Click this button if you wish to import accounts from a comma delimited text file. This button is identical to the Accounts » Importing » Import accounts from a comma delimited text file menu selection.

Templates
Click this button to open the Groups & Templates 576 dialog, from which you can manage the default settings for New Accounts 581 and control account group membership.

De-list
Select one or more accounts and then click this button if you wish to unsubscribe them from all Mailing Lists 186 hosted on the server. A box will open asking you to confirm the decision to remove the addresses from the lists.

BES
Select one or more accounts and then click this button to enable them for BlackBerry device synchronization 553. You will be asked to confirm your decision to enable the accounts. This has the same effect as separately opening each account's BlackBerry Enterprise Server screen and clicking the *Enable BlackBerry device synchronization* option.

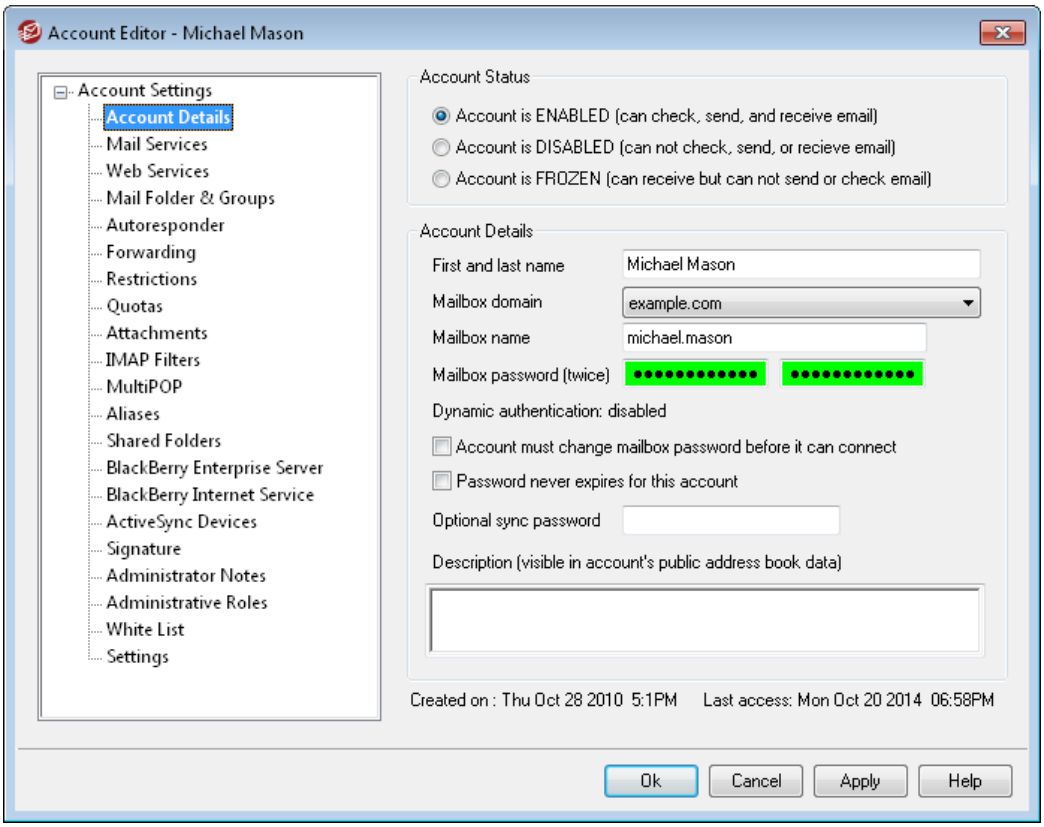
See:

Account Editor 521
New Accounts Template 581

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1 Account Editor

5.1.1.1 Account Details



Account Status

Account is ENABLED (can check, send, and receive email)
This is the default option; the account can check, send, and receive email.

Account is DISABLED (can not check, send, and receive email)
Select this options if you wish to disable all access to the account. The user will not be able to access the account by any means, nor will MDaemon accept mail for it. It will not be deleted, and it will still count toward the number of accounts used in your license's account limit, but MDaemon will operate as if the account doesn't exist.

Account is FROZEN (can receive but can not send or check email)
Select this options if you wish to allow the account to receive incoming messages but prevent it from being able to check or send messages. This is useful when, for example, you suspect the account has been hijacked. Freezing the account would prevent the malicious user from accessing its messages or using the account to send messages, but it would still be able to receive its incoming email.

Account Details

First and last name
Enter the user's first and last name here. When creating a new account, some of the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

fields on the various screens of the Account Editor (for example, *Mailbox name* and *Mail Folder*) will be automatically filled in while typing the first and last name and choosing the *Mailbox domain*. You can, however, change any of those default values. The first and last name field cannot contain " ! " or " | ".

Mailbox domain
Use this drop-down list box to specify the domain to which this account will belong and that will be used in its email address. MDaemon's Default Domain 121 will appear in the drop-down list by default.

Mailbox name
This is the portion of the account's email address that sets it apart from other accounts on the domain. The complete email address (i.e. [*Mailbox name*]@[*Mailbox domain*]) is used as the unique identifier for the account and as its login for POP3, IMAP, WorldClient, and so on. Email addresses cannot contain spaces or " ! " or "|" characters. Do not use "@" in this option. For example, use "frank.thomas" not "frank.thomas@".

Mailbox password (twice)
This is the password that the account will use when connecting to MDaemon to send or receive email via POP3 or IMAP, when authenticating during the SMTP process, or when using WorldClient, Remote Administration, or Outlook Connector. Both of these boxes will be highlighted in red if the passwords do not match or they violate the password restrictions 636. Otherwise they will be green.

If you are using Dynamic Authentication 644 for this account then you must enter two backslashes followed by the Windows domain to which the user belongs, rather than entering a password (for example, `\\ALTN` rather than `123Password`). Below the password fields there is a short statement to indicate whether dynamic authentication is enabled or disable for the account.

You should always provide a *Mailbox password* even if you do not wish to allow POP3/IMAP access to the mail account. In addition to mail session verification, the email address and *Mailbox password* values are used to allow remote account configuration and remote file retrieval. If you wish to prevent POP/IMAP access, use the options located on the Mail Services 525 screen. If you wish to prevent all access, then use the *Account is DISABLED* or *Account is FROZEN* options above.

Account must change mailbox password before it can connect
Check this box if you wish to require the account to change its *Mailbox password* before it can access POP, IMAP, SMTP, WorldClient, or Remote Administration. The user can connect to WorldClient or Remote Administration but will be required to change his or her password before proceeding. Note, however, that in order for users to be able to change their passwords via WorldClient or Remote Administration they must first be granted the "*...edit password*" web access permission on the Web Services 526 screen. After the password is changed this option will be deactivated.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Because changing the password may not be easy or possible for some users, you should exercise caution before activating this option.

Password never expires for this account
Check this box if you wish to exempt the account from the password expiration option located on the Passwords 636 dialog.

Optional sync password
Use this option if you wish to designate another password for the account to use when interacting with a synchronization server, such as SyncML 342 or ActiveSync 276 . If no sync password is assigned then the account's *Mailbox password* is used for sync connections. If both passwords are assigned then ActiveSync clients can use either password but SyncML clients must use the *Optional sync password*. For accounts using Dynamic Authentication 644, a sync password is necessary if the account is also using SyncML. SyncML does not support Dynamic Authentication.

Description
Use this text area if you wish to add a public description of the account.

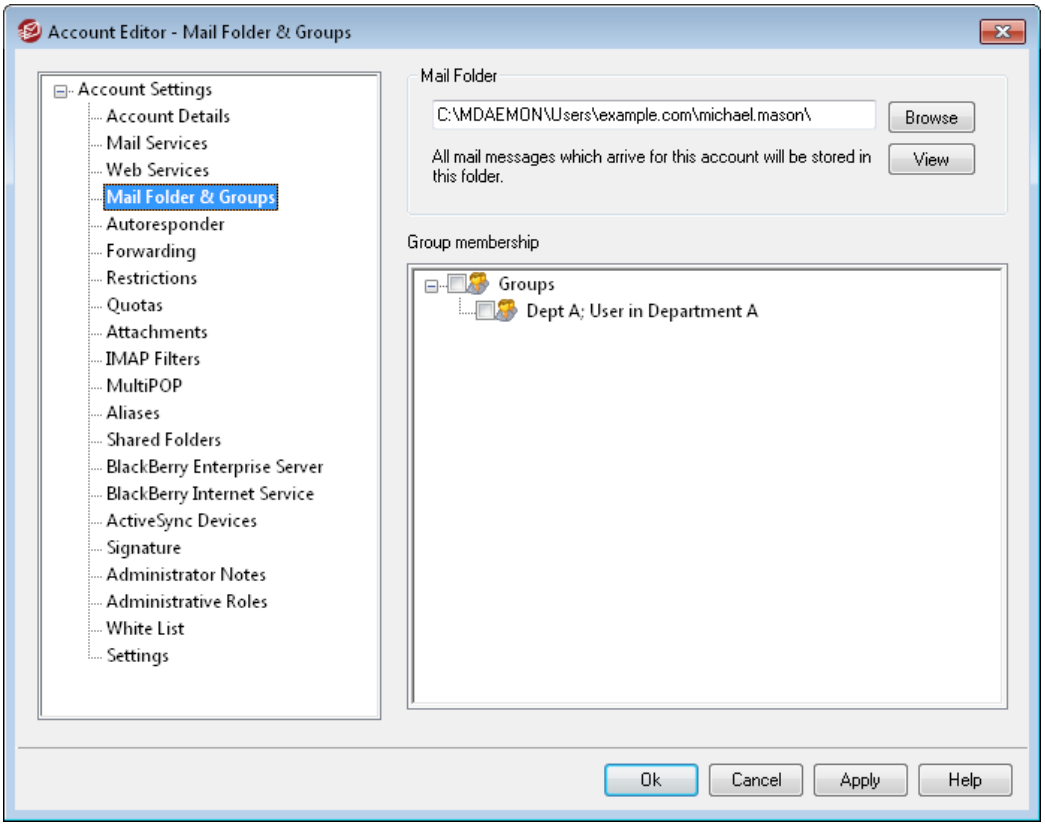
This description is included in the account's public contact record and is viewable by others. Do not include private or sensitive information in this field. For private notes or comments regarding this account, use the Administrator Notes 569 screen.

See:

Dynamic Authentication 644
Passwords 636
Account Editor » Web Services 526

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.2 Mail Folder & Groups



Mail Folder

Enter the folder where you wish to store this account's email messages. When creating a new account, the default location of this folder is based on the *Mail folder* setting designated on the New Accounts template 582.

View

Click this button to open the Queue/Stats Manager 665 to the user's *Mail Folder*.

Groups Membership

Use this box to add the account to one or more Groups 576. Check the box next to each group that you wish the account to join.

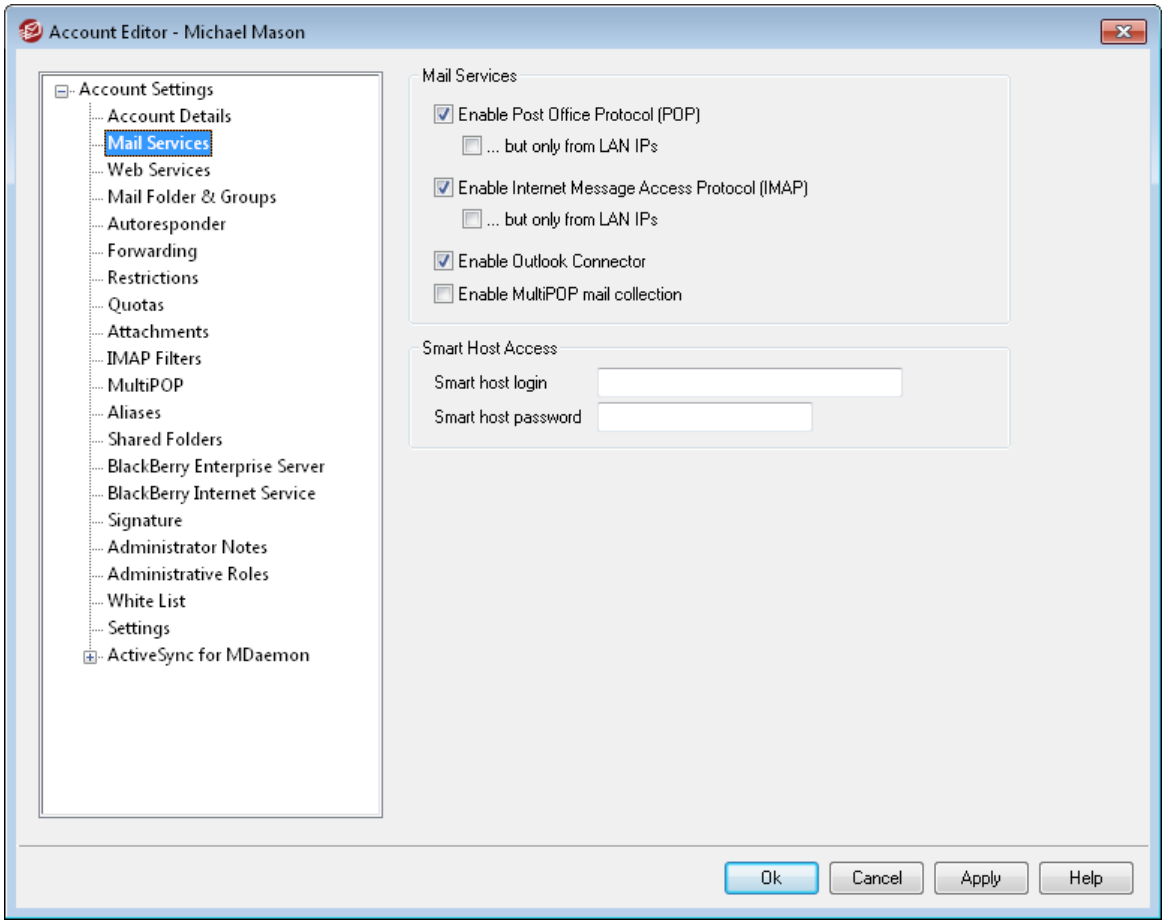
See:

New Accounts Template 582

Groups 576

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.3 Mail Services



The options on this screen govern which mail services the account is allowed to use: POP, IMAP, ActiveSync, MultiPOP, and Outlook Connector. Email access via WorldClient is controlled from the Web Services 526 screen. It also contains options for specifying optional Smart Host Access credentials for the account.

Mail Services

Enable Post Office Protocol (POP)
When this box is checked, the account's mail can be accessed via Post Office Protocol (POP). Virtually all email client software supports this protocol.

...but only from LAN IPs
Check this box if you wish to allow the account to be accessed via POP only when the user is connecting from a LAN IP address 514.

Enable Internet Message Access Protocol (IMAP)
When this box is checked, the account's mail can be accessed via Internet Message Access Protocol (IMAP). IMAP is more versatile than POP3, allowing email to be managed on the server and accessed using multiple clients. Most email client software supports this protocol. MDaemon Pro is required for IMAP support.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...but only from LAN IPs
Check this box if you wish to allow the account to be accessed via IMAP only when the user is connecting from a LAN IP address 514.

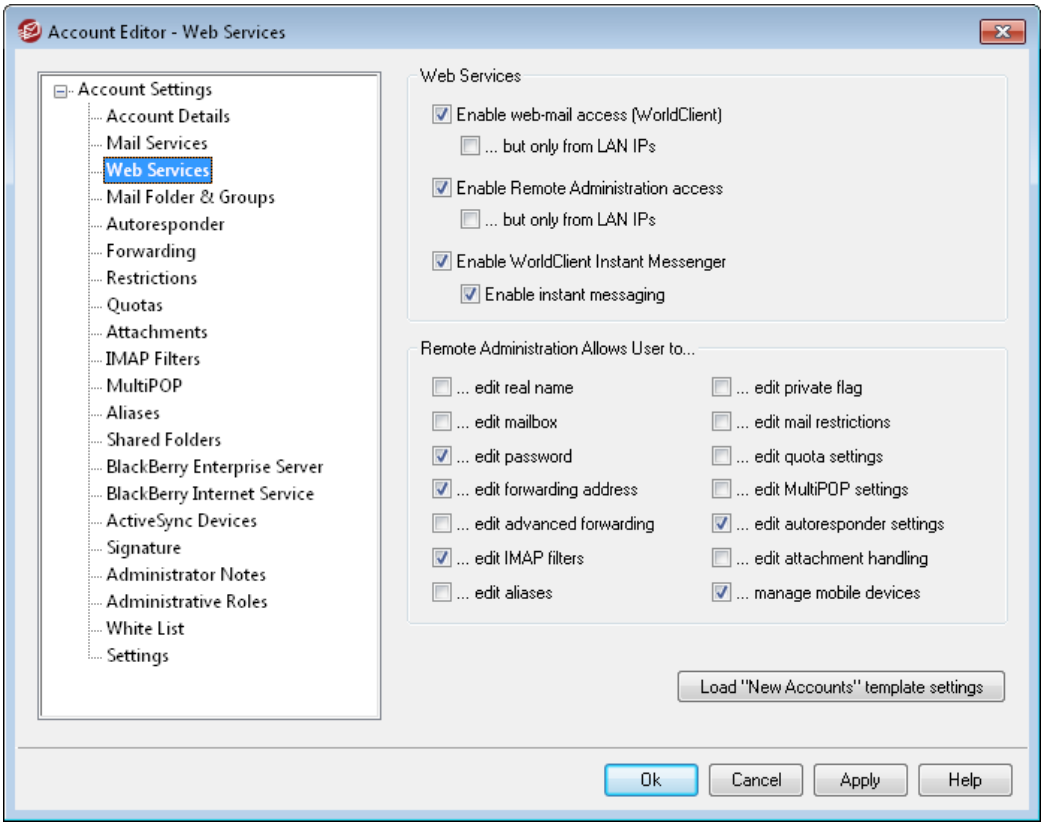
Enable Outlook Connector
Click this option if you wish to allow the account to share Microsoft Outlook folders using Outlook Connector for MDaemon 625. **Note:** this option will only be available when Outlook Connector is installed.

Enable MultiPOP mail collection
Check this box if you wish to allow the account to use MultiPOP 544. MultiPOP allows the user to collect mail from other email accounts, maintained on other mail servers.

Smart Host Access

Smart host login/password
If the *Allow per-account authentication* option is enabled on the Delivery 50 screen at Setup » Server Settings, and you wish to use per-account authentication with this account instead of using the credentials specified on that screen, then specify the account's optional smart host credentials here. If you do not wish to use per-account authentication for this account then leave these options blank.

5.1.1.4 Web Services



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Web Service

Enable web-mail access (WorldClient)
Enable this checkbox if you want the account to be able to access WorldClient 224, which enables users to access their email, calendars, and other features using a web browser.

...but only from LAN IPs
Check this box if you wish to allow the account access to WorldClient only when connecting from a LAN IP address 514.

Enable Remote Administration access
Check this box if you wish to grant the user permission to modify his or her account settings via Remote Administration 251. The user will only be able to edit those settings that you designate below.

When this feature is enabled and the Remote Administration server is active, the user will be able to log in to Remote Administration by pointing a browser to the designated MDaemon domain and port assigned to Remote Administration 252 (e.g. `http://example.com:1000`). He will first be presented with a sign-in screen and then a screen that contains the settings that he has been given permission to edit. All he needs to do is edit whatever settings he chooses and then click the *Save changes* button. He can then sign out and close the browser. If he has access to WorldClient then he can also access Remote Administration from the Advanced Options menu within WorldClient.

If the user is a Global or Domain Administrator (designated on the Account Editor's Administrative Roles 570 screen) he will see a different screen after he logs in to Remote Administration.

...but only from LAN IPs
Check this box if you wish to allow the account access to Remote Administration only when connecting from a LAN IP address 514.

Enable WorldClient Instant Messenger
Click this box if you wish to enable WCIM 225 support for this account.

Enable Instant Messaging
When WCIM support is enabled for the account, click this option is you also wish to enable support for WCIM's instant messaging system. When this checkbox is cleared, you will be able to access WCIM's other features, but not instant messaging.

Remote Administration Allows User to...

...edit real name
Enabling this feature will allow the user to modify the account's *First and last name* 521 setting.

...edit mailbox
Enabling this feature will allow the user to modify the account's *Mailbox name* 521.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Because the *Mailbox name* is part of the account's email address, which is the unique identifier and login value for the account, changing it means that the user will be changing his or her actual email address. This could result in any future messages directed to the old address being rejected, deleted, or the like.

...edit password
Click this checkbox if you wish to allow the user to modify the account's *Mailbox password*. For more on password requirements, see: Passwords 636.

...edit forwarding address
When this feature is enabled, the user will be able to modify the forwarding 533 address settings.

...edit advanced forwarding
When this feature is enabled, the user will be able to modify the *Advanced Forwarding Settings* 533.

...edit IMAP filters
Use this control to enable the user to create and manage his own IMAP Filters 541. This feature is only available in MDaemon PRO.

...edit aliases
Enable this option if you wish to allow the account holder to use Remote Administration to edit Aliases 546 associated with his or her account.

...edit private flag
This option governs whether or not the user will be permitted to use Remote Administration to edit the "*Account is private*" option located on the Account Editor's Settings 573 screen.

...edit mail restrictions
This checkbox controls whether or not the account will be able to edit the Inbound/Outbound mail restriction, located on the Restrictions 534 screen.

...edit quota settings
Click this checkbox if you wish to allow the account to modify the Quota 537 settings.

...edit MultiPOP settings
Click this checkbox if you wish to give the account permission to add new MultiPOP 544 entries and to enable/disable MultiPOP collection for those entries.

...edit autoresponder settings
Click this checkbox if you wish to give the user permission to add, edit, or delete Autoresponders 529 for his account.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...edit attachment handling
Check this box if you wish to allow the user to edit the account's attachment handling options, located on the Attachments 539 screen.

...manage mobile device
Click this option if you wish to allow the account holder to use Remote Administration to manage his or her device-specific settings, such as for BlackBerry and ActiveSync devices.

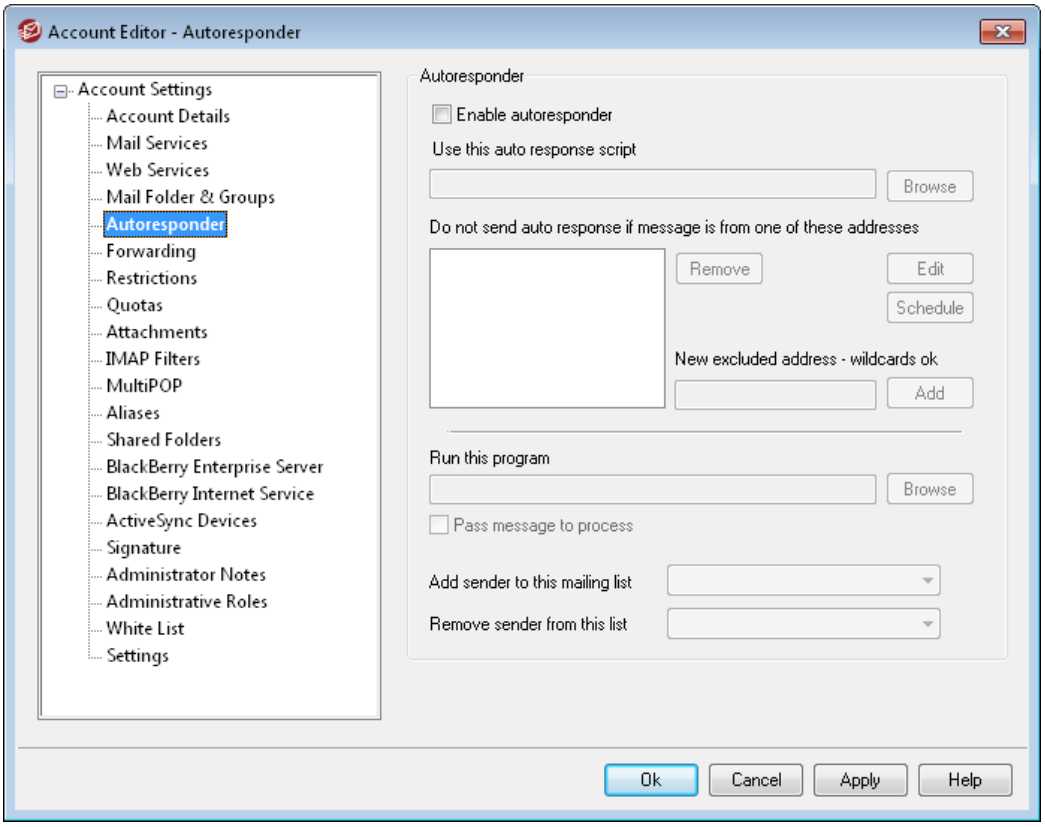
Load "New Accounts" template settings

Click this button to return the settings on this screen to the default values designated on the Web Services 587 screen of the *New Accounts* template.

See:

WorldClient 224
Remote Administration 251
Template Manager » Web Services 587

5.1.1.5 Autoresponder



Autoresponders are useful tools for causing incoming email messages to trigger certain events automatically, such as running a program, adding the sender to a mailing list, responding with an automatically generated message, and more. The most common use

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

of autoresponders is to reply to incoming messages automatically with a user-defined message stating that the recipient is on vacation, is unavailable, will reply as soon as possible, or the like. MDaemon users with web access 526 to WorldClient 224 or Remote Administration 251 can use the options provided to compose auto response messages for themselves and schedule the dates they will be in use. Finally, automated response messages are based on response scripts 621 (*.RSP files), which support a large number of macros. These macros can be used to cause much of the script's content to be generated dynamically, making autoresponders quite versatile.

Auto response events are always honored when the triggering message is from a remote source. However, for messages originating locally, autoresponders will only be triggered if you enable the *Autoresponders are triggered by intra-domain mail* option, located on the Autoresponders » Settings 620 screen. You can also use an option on that screen to limit auto response messages to one response per sender per day.

Autoresponder

Enable autoresponder
Enable this control to activate an autoresponder for the account. For more information on autoresponders see: Autoresponders 617.

Use this auto response script
This field is used to specify the path and filename of the response file (*.RSP) that will be processed and used to compose the message that will be returned to the message sender. Response scripts may contain macros that can be used to make response messages dynamic and automate much of their content. See, Creating Auto Response Scripts 621 for more information.

Do not send auto response if message is from one of these addresses
Here you can list addresses that you wish to be excluded from responses initiated by this autoresponder.

Occasionally auto response messages may be sent to an address that returns an auto response of its own. This can create a "ping-pong" effect causing messages to be continually passed back and forth between the two servers. If you encounter one of those addresses, enter it here to prevent that from happening. There is also an option located on the Autoresponders » Settings 620 screen, which can be used to limit auto response messages to one response per sender per day.

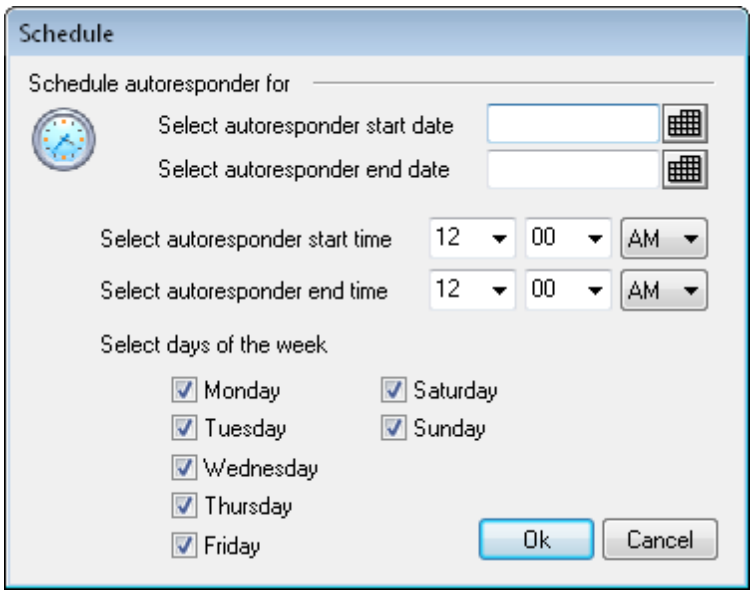
Remove
Click this button to delete any selected entries from the list of excluded addresses.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

New excluded address—wildcards okay
If you wish to add an address to the list of excluded addresses enter it here and then click the *Add* button.

Edit
Click this button to open and edit your selected Auto Response Script.

Schedule
Click this button to open the Schedule dialog on which you can set a start and end date and time for the Autoresponder, and set the days of the week for it to be active. Leave the Schedule blank if you want the Autoresponder to be active continually.



Run a Program

Run this program
Use this field to specify the path and filename to a program that you wish to run when new mail arrives for this account. Care must be taken to ensure that this program terminates properly and can run unattended. Optional command line parameters can be entered immediately following the executable path if desired.

Pass message to process
Select this option and the process specified in the *Run this Program* field will be passed the name of the triggering message as the first available command line parameter. When the autoresponder is set for an account that is forwarding mail to another location and **not** retaining a local copy in its own mailbox (see Forwarding 533) then this function will be disabled.

By default, MDaemon will place the name of the message file as the last parameter on the command line. You can override this behavior by using the `$MESSAGE$` macro. Use this macro in

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

place of where the message file name should be placed. This allows more flexibility in the use of this feature since a complex command line such as this will be possible: `logmail /e /j /message=$MESSAGE$ /q`.

Mailing Lists

Add sender to this mailing list
If a mailing list is entered in this field then the sender of the incoming message will be automatically added as a member of that mailing list. This is a handy feature for building lists automatically.

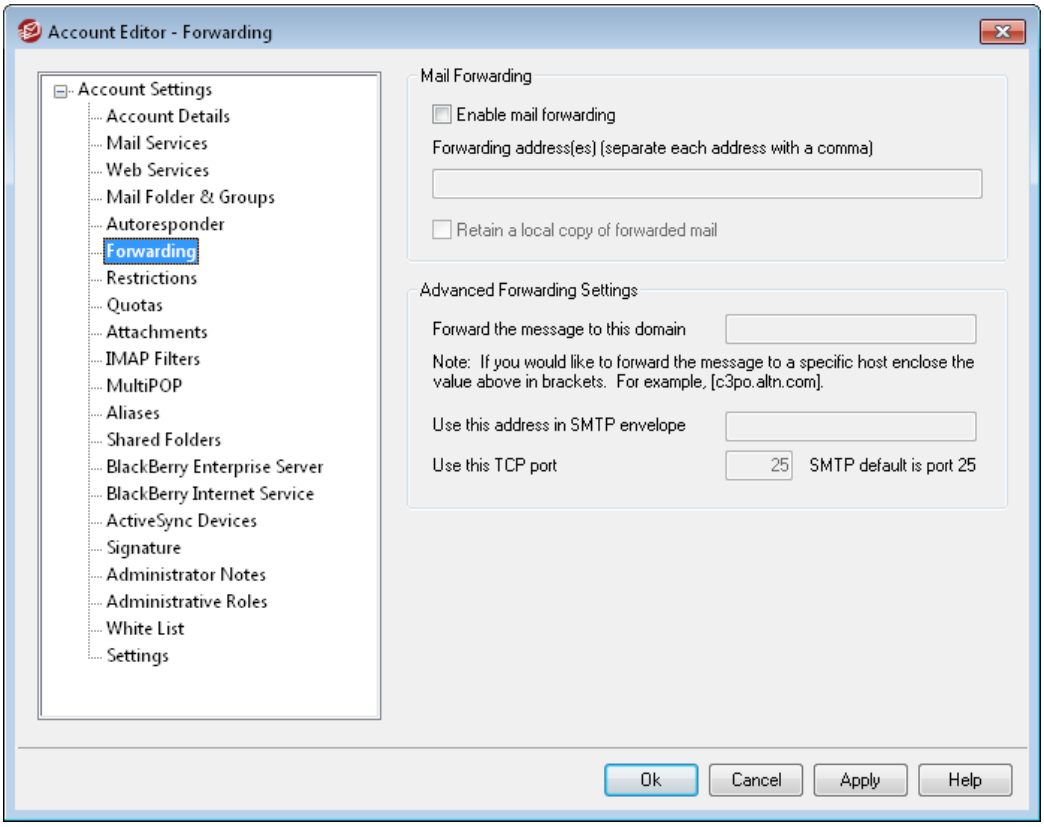
Remove sender from this mailing list
If a mailing list is entered in this field then the sender of the incoming message will be automatically removed from the specified mailing list.

See:

Autoresponders » Accounts 617
Autoresponders » White List 619
Autoresponders » Settings 620
Creating Auto Response Scripts 621

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.6 Forwarding



Mail Forwarding

Enable mail forwarding
Check this box if you wish to forward this account's incoming messages to the address or addresses specified in the *Forwarding addresses* option below. MDaemon users with web access 526 to WorldClient 224 or Remote Administration 251 can use the options provided to set the forwarding options for themselves rather than requiring an administrator to do so.

Forwarding addresses (separate each address with a comma)
Use this field to designate any email addresses to which you wish to forward copies of this account's incoming messages as they arrive. A copy of each new message arriving at the server will be automatically generated and forwarded to the addresses specified in this field, provided the *Enable mail forwarding* option above is checked. When forwarding to multiple addresses, separate each one with a comma.

Retain a local copy of forwarded mail
By default, a copy of each forwarded message is delivered normally to the local user's mailbox. If you uncheck this box then no local copy will be retained.

Advanced Forwarding Settings

Forward the message to this domain
If you wish to route the forwarded messages through a particular domain's MX

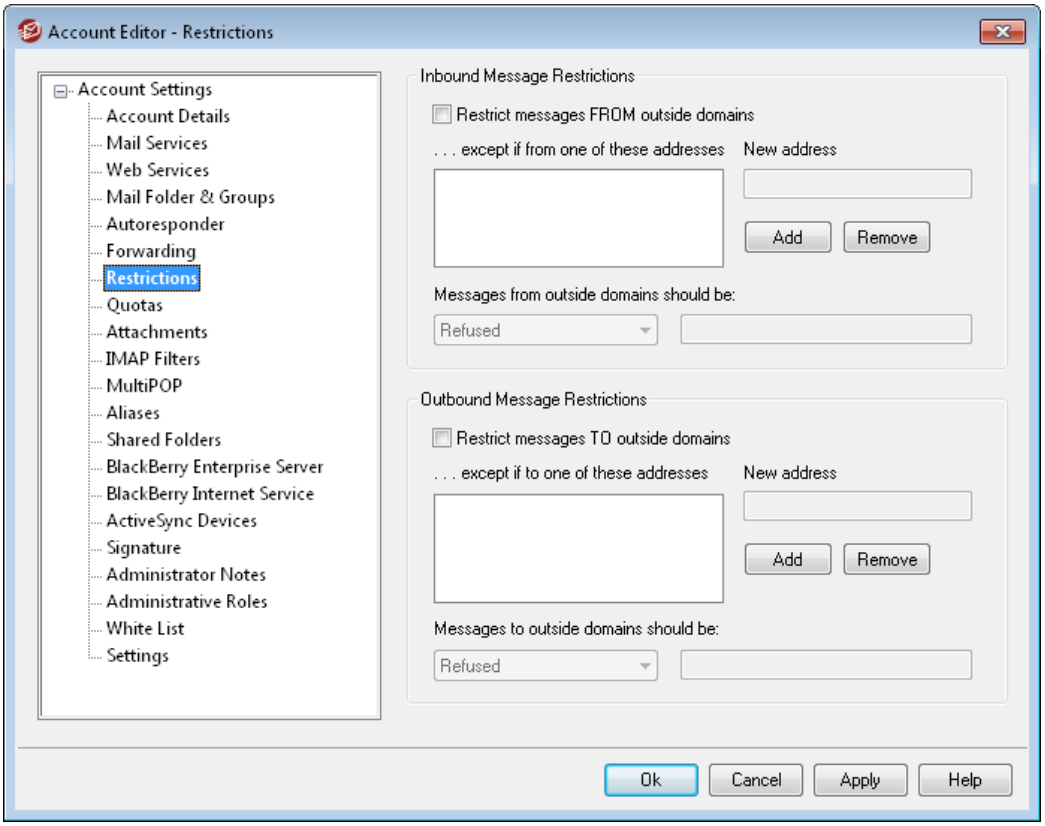
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

servers, then specify that domain here. If you wish to route the messages to a specific host, then enclose the value in brackets (e.g. [host1.example.com]).

Use this address in SMTP envelope
If an address is specified here, it will be used in the "MAIL From" statement sent during the SMTP session with the accepting host, instead of using the actual sender of the message. If you require an empty SMTP "MAIL From" statement (i.e. "MAIL FROM <>") then enter "[trash]" into this option.

Use this TCP port
MDaemon will send the forwarded messages using the TCP port specified here. The default SMTP port is 25.

5.1.1.7 Restrictions



Use the options on this screen to govern whether or not the account will be able to send or receive mail to or from non-local domains.

Inbound Message Restrictions

Restrict messages FROM outside domains
Click this checkbox to prevent this account from receiving email messages from non-local domains.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...except if from one of these addresses
Addresses specified in this area are exceptions to the Inbound Message Restrictions. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then no inbound messages from any address at altn.com would be restricted.

New address
If you wish to add an address exception to the Inbound Message Restrictions list then type it here and click the *Add* button.

Add
After entering an address into the *New address* option, click this button to add it to the exceptions list.

Remove
If you wish to remove an address from the restrictions list, select the address and then click this button.

Messages from outside domains should be...
The options in this drop-down list box govern what MDaemon will do with messages that are destined for this account but originate from a non-local domain. You may choose any of the following options:

Refused – Restricted messages will be refused by MDaemon.

Returned to sender – Messages from restricted domains will be returned to the sender.

Sent to postmaster – Messages that are restricted will be accepted but delivered to the postmaster instead of this account.

Sent to... – Messages that are restricted will be accepted but delivered to the address that you specify in the text box on the right.

Outbound Message Restrictions

Restrict messages TO outside domains
Click this checkbox to prevent this account from sending email messages to non-local domains.

...except if to one of these addresses
Addresses specified in this area are exceptions to the Outbound Message restriction. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then outbound messages to any address at altn.com would not be restricted.

New address
If you wish to add an address exception to the Outbound Message Restrictions list then type it here and click the *Add* button.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Add
After entering an address into the *New address* option, click this button to add it to the exceptions list.

Remove
If you wish to remove an address from the restrictions list, select the address and then click this button.

Messages to outside domains should be...
The options in this drop-down list box govern what MDaemon will do with messages that originate from this account but are destined for a non-local domain. You may choose any of the following options:

Refused – Restricted messages will be refused by MDaemon.

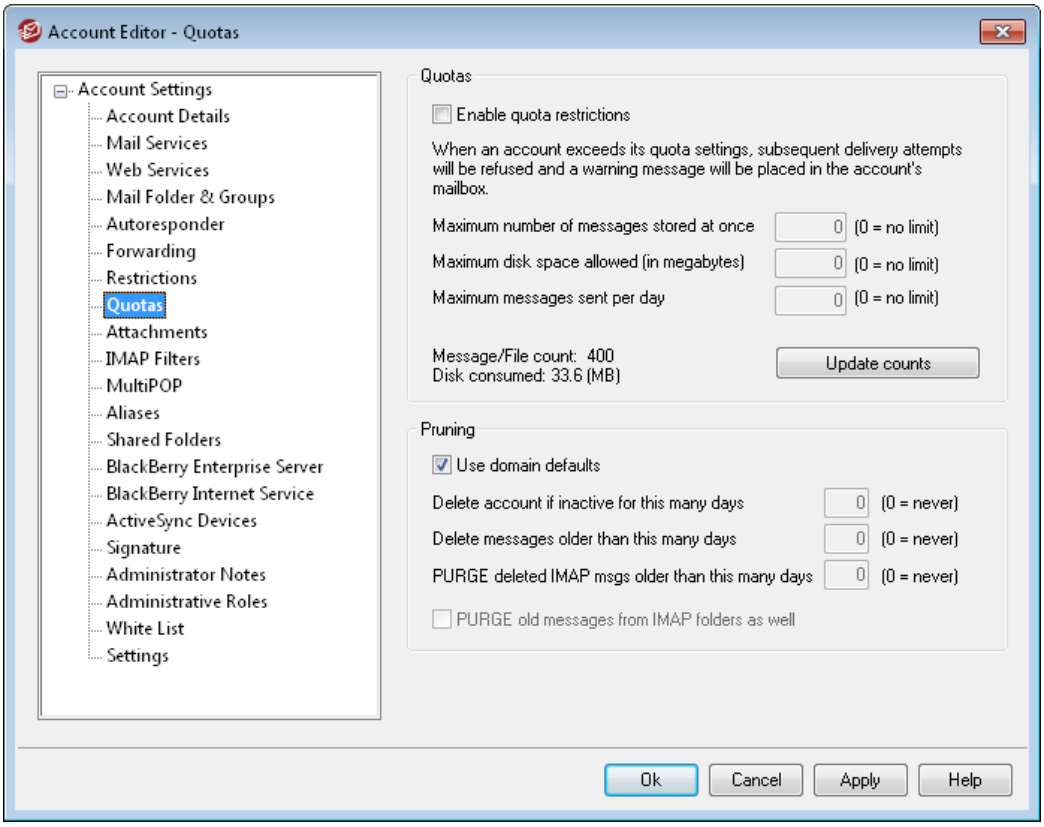
Returned to sender – Messages to restricted domains will be returned to the sender.

Sent to postmaster – Messages that are restricted will be accepted but delivered to the postmaster instead of the designated recipient.

Sent to... – Messages that are restricted will be accepted but delivered to the address that you specify in the text box on the right.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.8 Quotas



Quotas

Enable quota restrictions
Check this box if you wish to specify a maximum number of messages that the account can store, set a maximum amount of disk space that the account can use (including any file attachments in the account's Documents folder), or designate a maximum number of messages that the account can send via SMTP per day. If a mail delivery is attempted that would exceed the maximum message or disk space limitations, the message will be refused and an appropriate warning message will be placed in the user's mailbox. If a MultiPOP 544 collection would exceed the account's maximum a similar warning is issued and the account's MultiPOP entries are automatically switched off (but not removed from the database).

Use the *Send quota warning emails to accounts nearing the limit* option at "Accounts » Account Settings » Quotas 596" to cause a warning message to be sent when an account nears its quota limits. When the account exceeds a designated percentage value of either its *Maximum number of messages stored at once* or *Maximum disk space allowed* restriction, a warning message will be sent to the account at midnight. The message will list the account's number of stored messages, the size of its mailbox, and the percent used and remaining.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

> Further, if an existing warning is found in the account's mailbox it will be replaced with an updated message.

Maximum number of messages stored at once
Use this option to designate the maximum number of messages that can be stored for the account. Using "0" in the option means there will be no limit to the number of messages permitted.

Maximum disk space allowed (in megabytes)
Use this option to designate the maximum amount of disk space that the account can use, including any file attachments that may be stored in the account's Documents folder. Using "0" in the option mean there will be no limit to the amount of disk space that the account can use.

Maximum messages sent per day
Use this option to designate the maximum number of messages that the account can send per day via SMTP. If the account reaches this limit then new mail from the account will be refused until the counter is reset at midnight. Use "0" in the option if you do not wish to limit the number of messages the account can send.

Update counts
Click this button to update the *Message/File count* and *Disk consumed* statistics displayed to the left.

Pruning

The options in this section are used to designate when or if this account will be deleted by MDaemon if it becomes inactive. You can also designate whether or not old messages belonging to the account will be deleted after a certain amount of time. Each day at midnight, MDaemon will remove all messages that have exceeded the time limits stated, or it will delete the account completely if it has reached the inactivity limit.

Use domain defaults
The default Pruning settings are domain-specific and located on the Domain Manager's Settings 140 screen. If you wish to override the domain defaults for this account, clear this checkbox and set the desired values in the options below.

Delete account if inactive for this many days (0 = never)
Specify the number of days that you wish to allow the account to be inactive before it will be deleted. A value of "0" in this control means that the account will never be deleted due to inactivity.

Delete messages older than this many days (0 = never)
This is the number of days that any given message may reside in the account's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

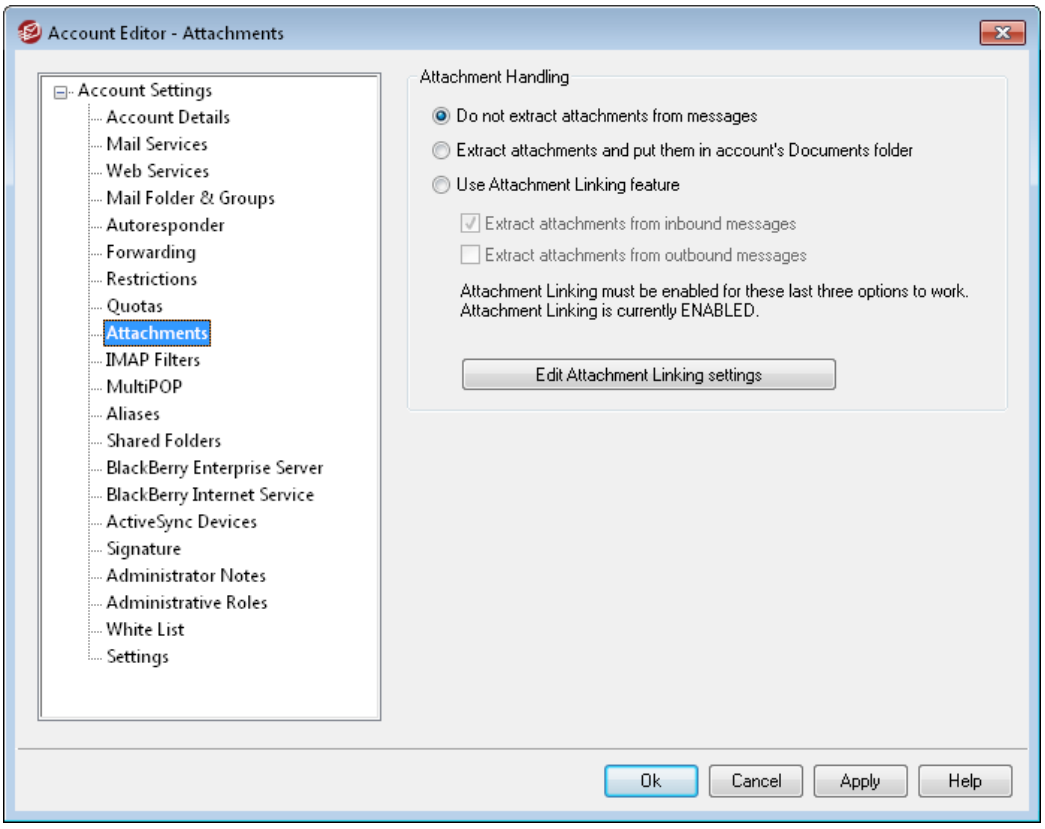
PURGE deleted IMAP msgs older than this many days (0 = never)
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in this user's folders. Messages flagged for deletion longer than this number of days will be purged. A value of "0" means that messages flagged for deletion will never be purged due to their age.

PURGE old messages from IMAP folders as well
Click this checkbox if you want the "*Delete messages older than...*" option to apply to messages in IMAP folders as well. When this option is disabled, messages contained in IMAP folders will not be deleted, regardless of their age.

See:

Template Manager » Quotas 596
Account Settings » Quotas 638

5.1.1.9 Attachments



Attachment Handling

This screen is used to control whether or not MDaemon will extract attachments from this account's email messages. You can use the Template Manager 599 to designate the default settings for these options.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Do not extract attachments from messages
If this option is selected, attachments will not be extracted from the account's messages. Messages with attachments will be handled normally, leaving the attachments intact.

Extract attachments and put them in account's Documents folder
If set, this option causes MDaemon to automatically extract any Base64 MIME embedded file attachments found within incoming mail messages for this account. Extracted files are removed from the incoming message, decoded, and placed in the account's Documents folder. A note is then placed within the body of the message, stating the names of the files that were extracted. This option does not provide a link to the stored attachments, but users can use WorldClient 224 to access their Documents folder.

Use Attachment Linking feature
Select this option if you wish to use the Attachment Linking feature for inbound or outbound messages with attachments.

If this option is selected but the Attachment Linking feature is disabled on the Attachment Linking 262 dialog, then attachments will not be extracted.

Extract attachments from inbound messages
When this option is enabled, attachments will be extracted from the account's incoming messages and stored in the location designated on the Attachment Linking 262 dialog. URL links are then placed within the body of the message, which the user can then click to download the files. For security these URL links do not contain direct file paths. Instead they contain a unique identifier (GUID) that the server uses to map the file to the actual path. This GUID map is stored in the `AttachmentLinking.dat` file. This option is enabled by default.

Extract attachments from outbound messages
Check this box if you wish to use the Attachment Linking feature to extract attachments from the account's outbound messages. When the account sends an email, Attachment Linking will extract the file, store it, and replace it with a URL to download the file.

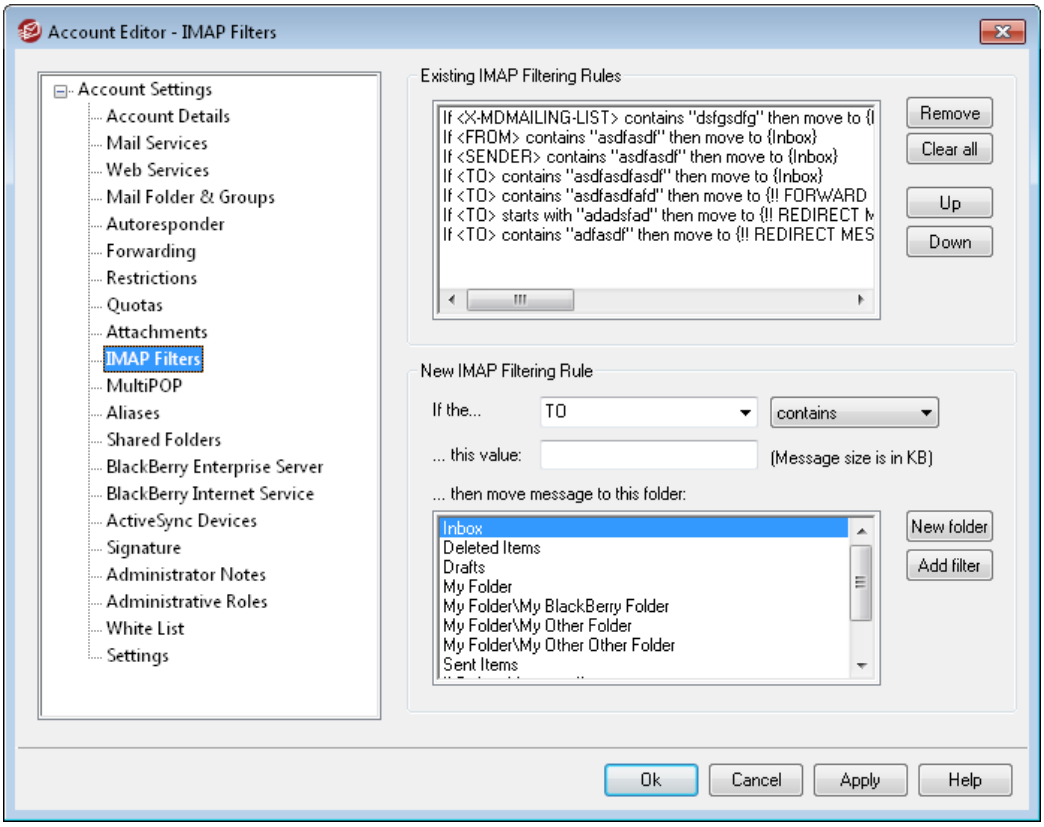
Edit Attachment Linking settings
Click this button to open the Attachment Linking 262 dialog.

See:

Attachment Linking 524
Template Manager » Attachments 599

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.10 IMAP Filters



With MDaemon, IMAP and WorldClient 224 users can have their mail routed automatically to specific folders on the server by using filters. Similar to the Content Filters 364, MDaemon will examine the headers of each of the account's incoming messages and then compare them to the account's filters. When a message for the account matches one of its filters, MDaemon will move it to the folder specified in that filter. This method is much more efficient (for both the client and server) than attempting to filter the messages at the client, and since some mail clients do not even support local message rules or filtering, mail filters provide this option to them.

Administrators can create filters via the IMAP Filters screen of the Account Editor, or by using Remote Administration 251. However, you can also grant your users permission to create and manage filters for themselves from within WorldClient or Remote Administration. These permissions are set on the Web Services 526 screen.

Existing IMAP filter rules

This box displays the list of all filters that have been created for the user's account. Filters are processed in the order in which they are listed until a match is found. Therefore, as soon as a message matches one of the filters it will be moved to the folder specified in that filter and then filter processing for that message will cease. Use the *Up* and *Down* buttons to move filters to different positions in the list.

Remove
Click a filter in the list and then click *Remove* to delete it from the list.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Clear all
Click this button to delete all of the user's filters.

Up
Click a filter in the list and then click this button to move it to a higher position in the list.

Down
Click a filter in the list and then click this button to move it to a lower position in the list.

New IMAP Filtering Rule

If the... [message header/Size]
Choose "*Message Size*" or a header from this drop-down list box, or type a header into the box if the desired header is not listed. When a header is designated, MDaemon will scan that header in all of the account's incoming messages for the text contained in the "*this value*" box below. Then, based upon the type of comparison being made, it will determine which messages should be moved to the filter's specified folder.

Comparison-type
Use this drop-down list to choose the type of comparison that will be made to the message's header or size indicated in the filter. MDaemon will scan the specified header for the text contained in the "*this value*" field (or compare the message's size to that value) and then proceed based upon this option's setting —does the message size or header's complete text match exactly, not match exactly, contain the text, not contain it at all, start with it, and so on.

...this value
Enter the text that you want MDaemon to search for when scanning the message header that you have specified for the filter. When the filter is set to check the message's size, set this value to the desired number of KB.

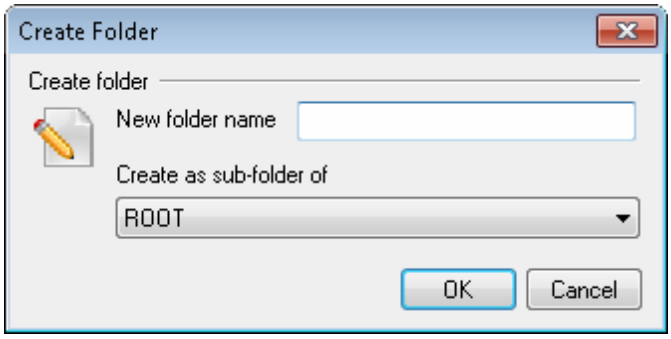
...then move message to this folder
After specifying the various parameters for the filter, click the folder that you want messages matching it to be moved to and then click the *Add filter* button to create the filter. This list also contains the following three special entries: "*!!Delete Message!!*," "*!!Redirect Message!!*," and "*!!Forward Message!!*."

- **!! Delete Message !!** – Choose your filter values, click this option in the folder list, and then click *Add filter* to create a filter that will cause a message to be deleted when it matches the filter's conditions.
- **!! Redirect Message !!** – Choose your filter values, click this option in the folder list, click *Add filter*, and then enter an Email address. This will create a filter that will cause a message that meets the filter's conditions to be redirected to the designated email address. No changes to the message headers or body will be made. The only thing changed is the SMTP envelope recipient.
- **!! Forward Message !!** – Choose your filter values, click this option in the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

folder list, click *Add filter*, and then enter an Email address. This will create a filter that will cause a message that meets the filter's conditions to be forwarded to the designated email address. A new message will be created and sent, with the Subject header and body content taken from the original message.

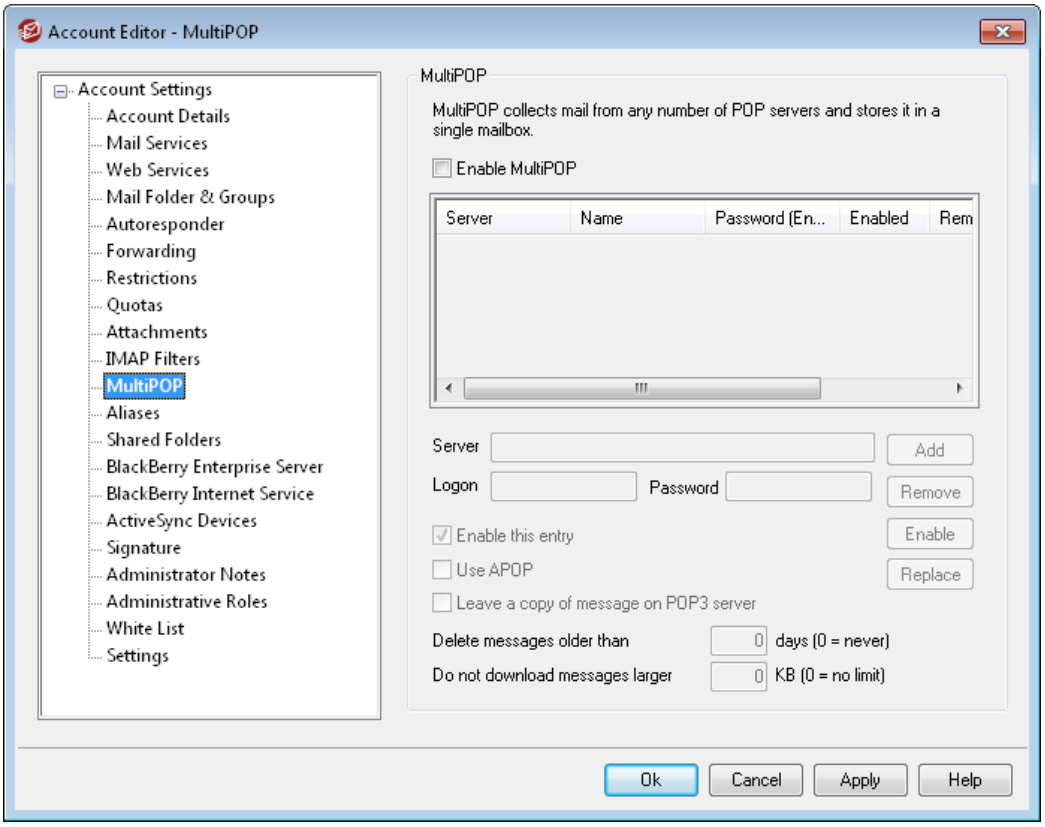
New folder
Click this button to create a new folder. This will open the Create Folder dialog on which you will assign a name for the folder. If you want it to be a subfolder of an existing folder then choose the folder from the drop-down list.



Add filter
When you are finished making your choices for a new filter, click this button to add it to the list.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.11 MultiPOP



The MultiPOP feature allows you to create an unlimited number of POP3 host/user/password combinations for collection of mail messages from multiple sources. This is useful for your users who have mail accounts on multiple servers but would prefer to collect and pool all their email together in one place. Before being placed in the user's mailbox, MultiPOP collected mail is first placed in the local queue so that it can be processed like other mail having Autoresponders and Content filters applied to it. The scheduling options for MultiPOP are located at: Setup » Event Scheduling » Mail Scheduling » MultiPOP Collection 272.

Enable MultiPOP
Check this box to enable MultiPOP processing for this account.

Creating or Editing a MultiPOP Entry

Server
Enter the POP3 server from which you wish to collect mail.

Logon
Enter the POP3 username or login name that is associated with the mail account on the server specified above.

Password
Enter the POP3 or APOP password used for accessing the mail account on the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

specified server.

Use APOP
Click this checkbox if you want the MultiPOP entry to use the APOP method of authentication when retrieving mail from its corresponding host.

Leave a copy of message on POP3 server
Click this checkbox if you want to leave a copy of collected messages on the server. This is useful when you plan to retrieve these messages again at a later time from a different location.

Delete messages older than [XX] days (0 = never)
This is the number of days that a message can remain on the MultiPOP host before it will be deleted. Use "0" if you do not wish to delete older messages.

Don't download messages larger than [XX] KB (0 = no limit)
Enter a value here if you wish to limit the size of messages that may be downloaded.

Add
After entering all of the information for the new MultiPOP entry, click this button to add it to the list.

Remove
If you wish to delete one of your MultiPOP entries, select the desired entry and then click this button.

Enable/disable
Clicking this button toggles the state of the selected MultiPOP entries, giving you control over whether MDaemon will collect mail for this entry or skip over it when it performs its MultiPOP processing.

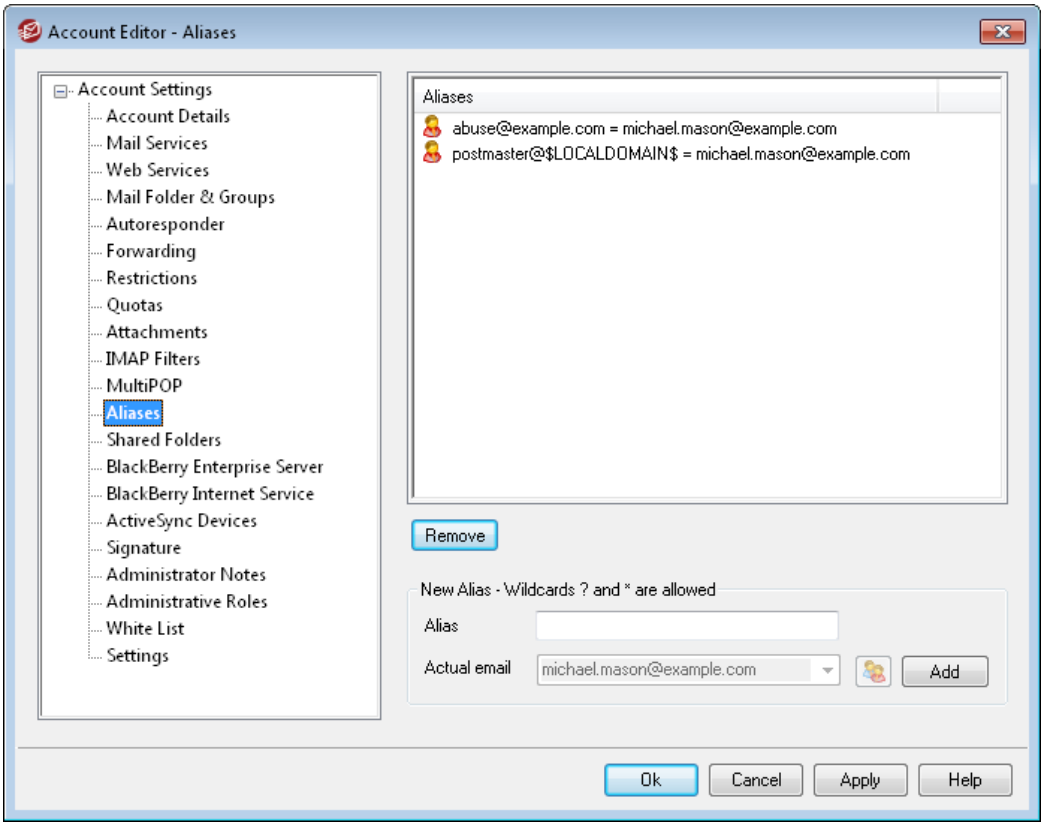
Replace
To edit an entry, click the entry in the list, make any desired changes, and click this button to save the changes to the entry.

See:

Event Scheduling » MultiPOP Collection 272

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.12 Aliases



This screen lists all address aliases[613] associated with the account, and can be used to add or remove them.

Removing an Alias

To remove an alias from the account, select the alias in the list and then click **Remove**.

Adding an Alias

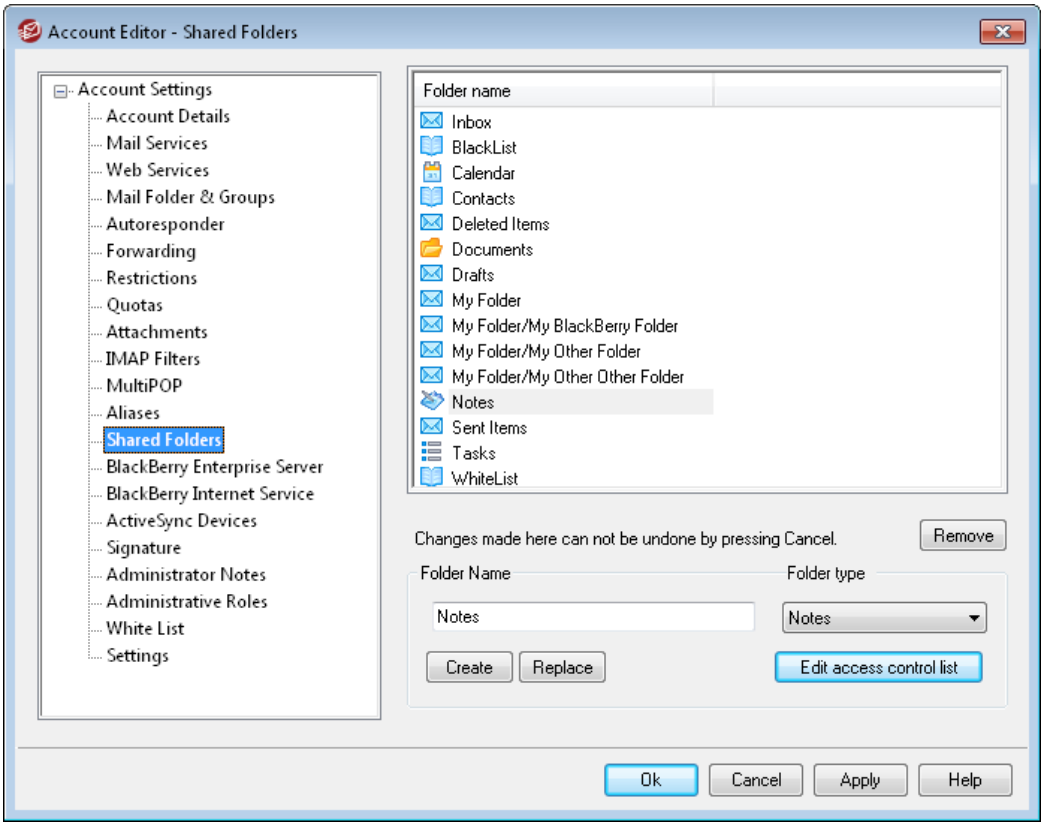
To add a new alias to the account, in the *Alias* box type the address that you wish to associate with the account and then click **Add**. The wildcards "?" and "*" are permitted, representing single characters and single words, respectively.

See:

Account Settings » Aliases[613]

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.13 Shared Folders



This screen is only available when the *Enable public folders* option is enabled on the Public & Shared Folders 87 screen, located at Setup » Server Settings » Public & Shared folders. Public Folders can be managed from the Public Folder Manager 218.

This top section displays all of the user's IMAP Folders and can be used to share access to them with other MDaemon users or Groups 576. When the account is first created, this area will only have the Inbox listed until you use the *Folder name* and *Create* options (or the options on IMAP Filters 541) to add folders to it. Subfolders in this list will have the folder and subfolder names separated by a slash.

Remove
To remove a Shared IMAP folder from the list, select the desired folder and then click the *Remove* button.

Folder name
To add a new folder to the list, specify a name for it in this option and click *Create*. If you want the new folder to be a subfolder of one of the folders in the list, then prefix the new folder's name with the parent folder's name and a slash. For example,

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

if the parent folder is "My Folder" then the new subfolder name would be "My Folder/My New Folder". If you don't want it to be a subfolder then name the new folder "My New Folder" without the prefix.

Folder type
Use this drop-down list to choose the type of folder you wish to create: Mail, Calendar, Contacts, and so on.

Create
After specifying a folder's name click this button to add the folder to the list.

Replace
If you wish to edit one of the Shared Folders, click the entry, make the desired change, and then click *Replace.*

Edit access control list
Choose a folder and then click this button to open the Access Control List 220 dialog for that folder. Use the Access Control List to designate the users or groups that will be able to access the folder and the permissions for each user or group.

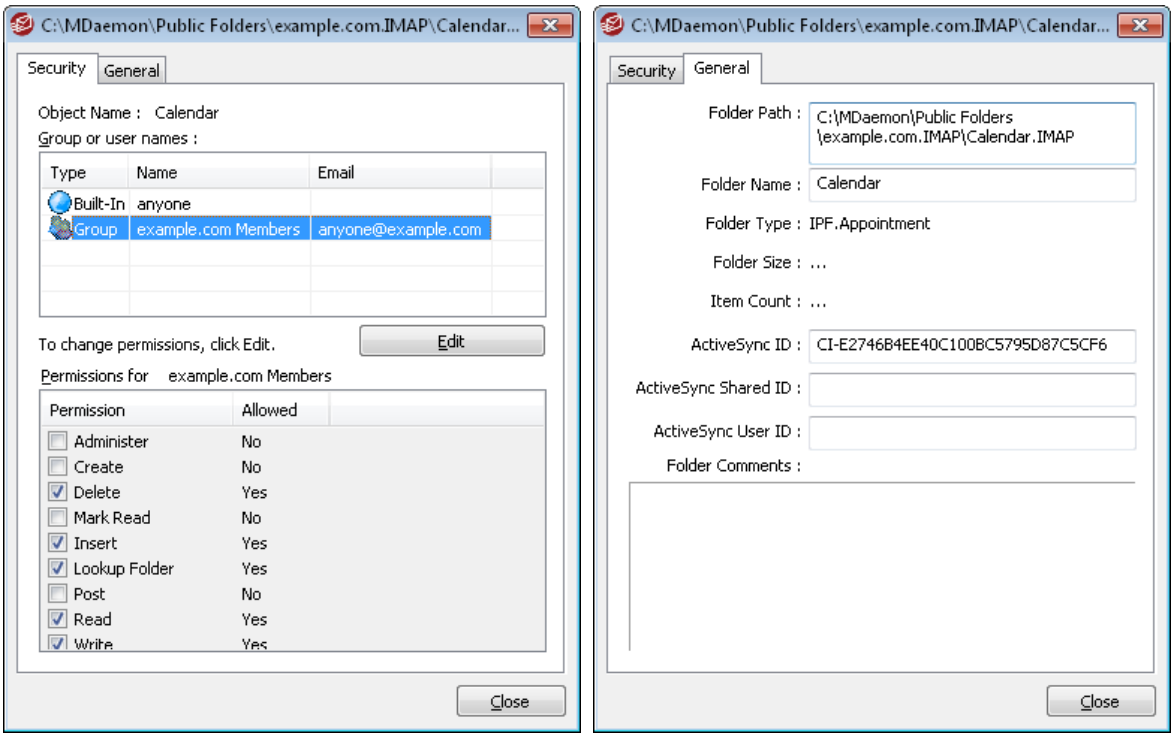
See:

Access Control List 220
Public Folder Manager 218

5.1.1.13.1 Access Control List

The Access Control List (ACL) is used for setting user or group access permissions for your public and shared folders 84. It is accessed from the *Edit ACLs* button on the Public Folder Manager 218 or the *Edit access control list* button on Account Editor's Shared Folders 547 screen.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Security

This tab displays the list of groups or users associated with the folder and the specific access permissions granted to each. Select a group or user in the list to display its permissions[221] for review in the Permissions window below. To edit the permissions, click **Edit**[221].

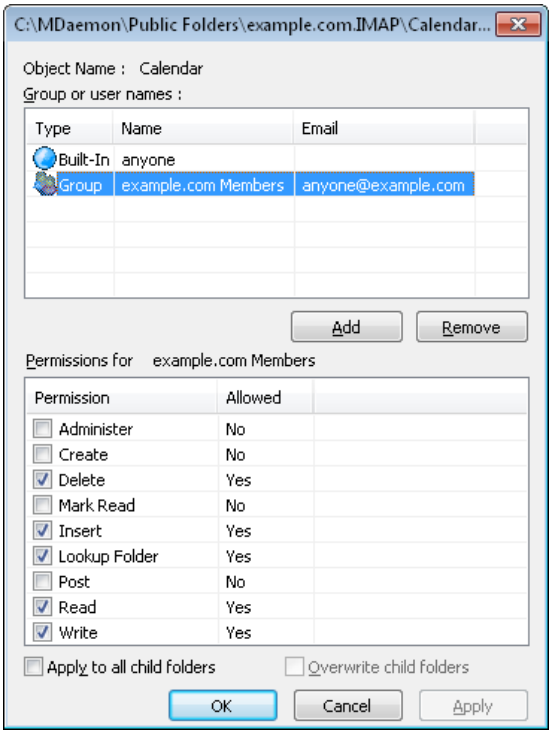
General

This tab displays the folder's properties, such as its path, name, type, size, and so on.

ACL Editor

Click **Edit** on the ACL's Security tab to open the ACL Editor for modifying access permissions.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Object Name
This is the name of the object or folder to which the ACL permissions will apply.

Group or user names
These are the groups or users to which some level of access permissions may have been granted. Select a group or user to display its permissions in the *Permissions for <group or user>* window below. Check the box next to any access permission that you wish to grant to the group or user.

Add
To grant access permissions to a group or user not listed above, click **Add** 222.

Remove
To remove a group or user, select its entry in the list above and click **Remove**.

Permissions for <group or user>
Check the box next to any access permission that you wish to grant to the group or user selected above.

You can grant the following access control permissions:

Administer – user can administer the ACL for this folder.

Create – user can create sub-folders within this folder.

Delete – user can delete items from this folder.

Mark Read – user can change the read/unread status of messages in this

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

folder.

Insert – user can append and copy items into this folder.

Lookup Folder – user can see this folder in his personal list of IMAP folders.

Post – user can send mail directly to this folder (if folder allows).

Read – user can open this folder and view its contents.

Write – user can change flags on messages in this folder.

Apply to all child folders
Check this box if you wish to apply this folder's access control permissions to any sub-folders it currently contains. This will add the folder's user and group permissions to the child folders, replacing them when there are any conflicts. It will not, however, delete any other user or group permissions that currently have access to those folders.

Example,

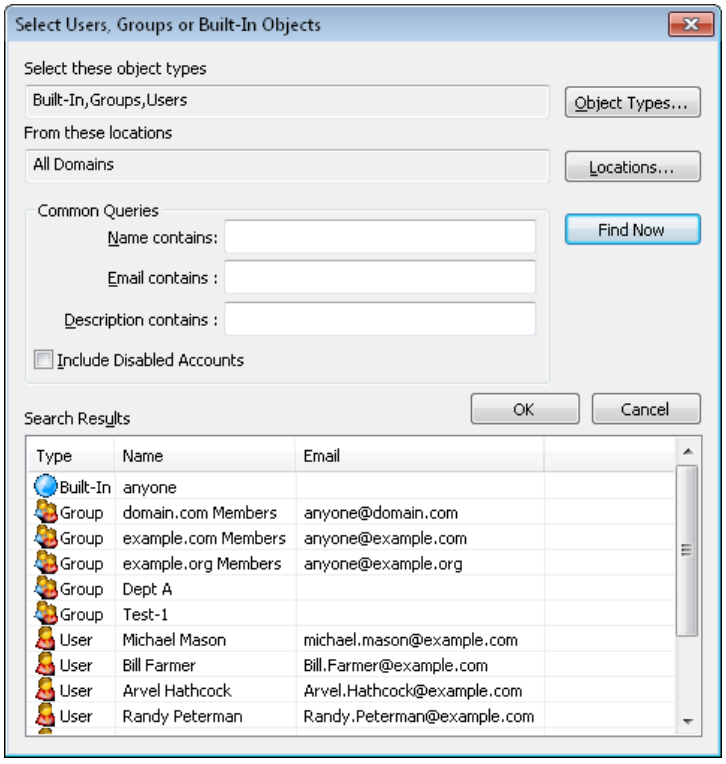
The parent folder grants certain permissions to `User_A` and `User_B`. The child folder grants permissions to `User_B` and `User_C`. This option will add `User_A` permissions to the child folder, replace the child folder's `User_B` permissions with those from the parent folder, and do nothing to the `User_C` permissions. Therefore the child folder will then have `User_A`, `User_B`, and `User_C` permissions.

Overwrite child folders
Check this box if you wish to replace all child folder access permissions with the parent folder's current permissions. The child folder permissions will then be identical to the parent folder.

Adding a Group or User

Click **Add** on the ACL Editor if you wish to add another group or user to the Access Control List. This opens the Add Group or User screen that you can use to search for them and then add them.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



Select these object types
Click **Object Types...** to select the object types that you wish to search for the groups or users you wish to add. You can select: Built-In, Groups, and Users.

From these locations
Click **Locations...** to select the domains that you wish to search. You can select all of your MDaemon domains or specific domains.

Common Queries
Use the options in this section to narrow your search by specifying all or part of the user's name, email address, or the contents of the account's Description 521. Leave these fields blank if you want the search results to contain every group and user that matches the Object Types and Locations specified above.

Include Disabled Accounts
Check this box if you wish to include disabled accounts 521 in your search.

Find Now
After you have specified all of your search criteria, click **Find Now** to perform the search.

Search Results
After performing the search, select any desired groups or users in the Search Results and click **OK** to add them to the ACL. To select more than one group or user, hold down the Ctrl key when selecting them.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

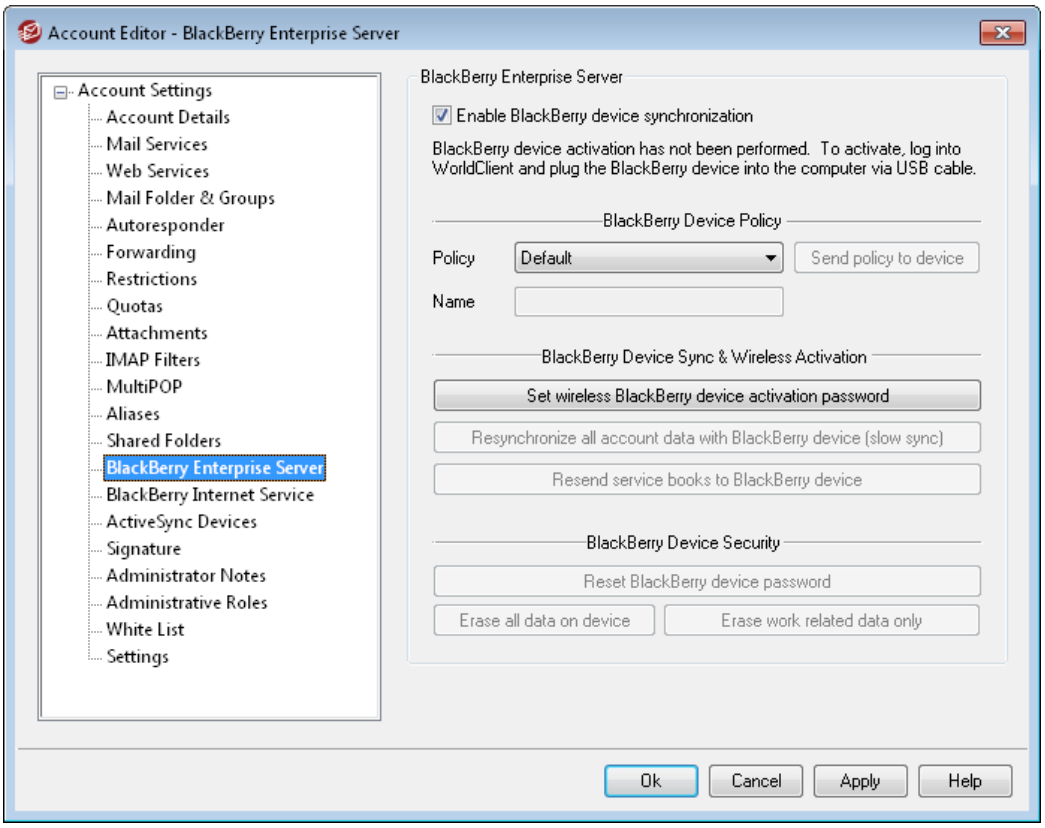
Access rights are controlled through MDaemon's support for Access Control Lists (ACL). ACL is an extension to the Internet Message Access Protocol (IMAP4), which makes it possible for you to create an access list for each of your IMAP message folders, thus granting folder access rights to other users who also have accounts on your mail server. If your email client doesn't support ACL you can still set the permissions via the controls on this dialog.

ACL is fully discussed in RFC 2086, which can be viewed at: http://www.rfc-editor.org/rfc/rfc2086.txt.

See:

Public Folder Manager 218
Public Folders Overview 84
Public & Shared Folders 87
Account Editor » Shared Folders 547
Mailing List » Public Folders 208

5.1.1.14 BlackBerry Enterprise Server



Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

The options on this screen govern BlackBerry Enterprise Server settings for the specific account and allow you to perform several actions regarding the account's activated BlackBerry device.

BlackBerry Enterprise Server is not available in some countries and regions.

Enable BlackBerry device synchronization

Click this checkbox to enable the account for BlackBerry device synchronization. BlackBerry enabled accounts appear on the BlackBerry Enterprise Server » Devices 328 screen and can activate a BlackBerry device via USB cable in WorldClient or over the air (OTA) from the device itself (not all devices support OTA activation).

After a device is activated, its PIN, Platform version, Phone model, and Number will be listed in this section.

After an account is enabled for BlackBerry device synchronization, the BlackBerry Enterprise Server database will begin storing information about the account's messages and data so that it can be synchronized 332 with a BlackBerry device when the device is activated. All messages that have been processed for the account since being BlackBerry enabled will be synchronized with the device when it is activated.

If you disable this option then all BlackBerry Enterprise Server data related to the account will be deleted. If you BlackBerry enable the account again then it will start storing data again, and the device will have to be reactivated.

BlackBerry Device Policy

Policy

Choose the policy 319 from the drop-down list that you want the device to use when it is activated.

Name

This is the name of the account as it will appear on the activated device (for example, "Desktop," "MDaemon," "Company" or the like).

Send policy to device

If the device is already activated and you wish to send a new policy to it, select the policy from the drop-down list and click this button.

BlackBerry Device Sync & Wireless Activation

Set wireless BlackBerry Device Activation password

To set a wireless BlackBerry Device Activation password for the account, click this button, enter a password, and click **OK**. The user can then enter the account's

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

email address and BlackBerry Device Activation password on the device's Enterprise Activation screen to activate it OTA. Not all devices can be activated wirelessly.

Resynchronize all account data with BlackBerry device (slow sync)
Click this button and then click **OK** on the confirmation dialog if you wish to resynchronize all account data with the device. This is commonly called "slow sync" and ensures that the data on the BlackBerry device matches what is in MDaemon. Depending on the amount of data, this can take several minutes to complete. When slow sync starts it will run in the background until finished. There is an option located on the BlackBerry Enterprise Server » Devices 328 screen that can be used to resynchronize **all** activated BlackBerry devices. See BlackBerry Enterprise Server » Settings 330 for more BlackBerry Enterprise Server synchronization options.

Resend service books to BlackBerry device
If you need to resend the service books to the account's BlackBerry device, click this button and then click **Yes** on the confirmation dialog.

BlackBerry Device Security

Reset BlackBerry device password
If you wish to remotely reset the device's password, click this button, enter a password, and click **OK**.

Erase all data on device
If you need to erase all data on the BlackBerry device remotely, such as when the device is lost or stolen, click this button and click **Yes** on the confirmation dialog.

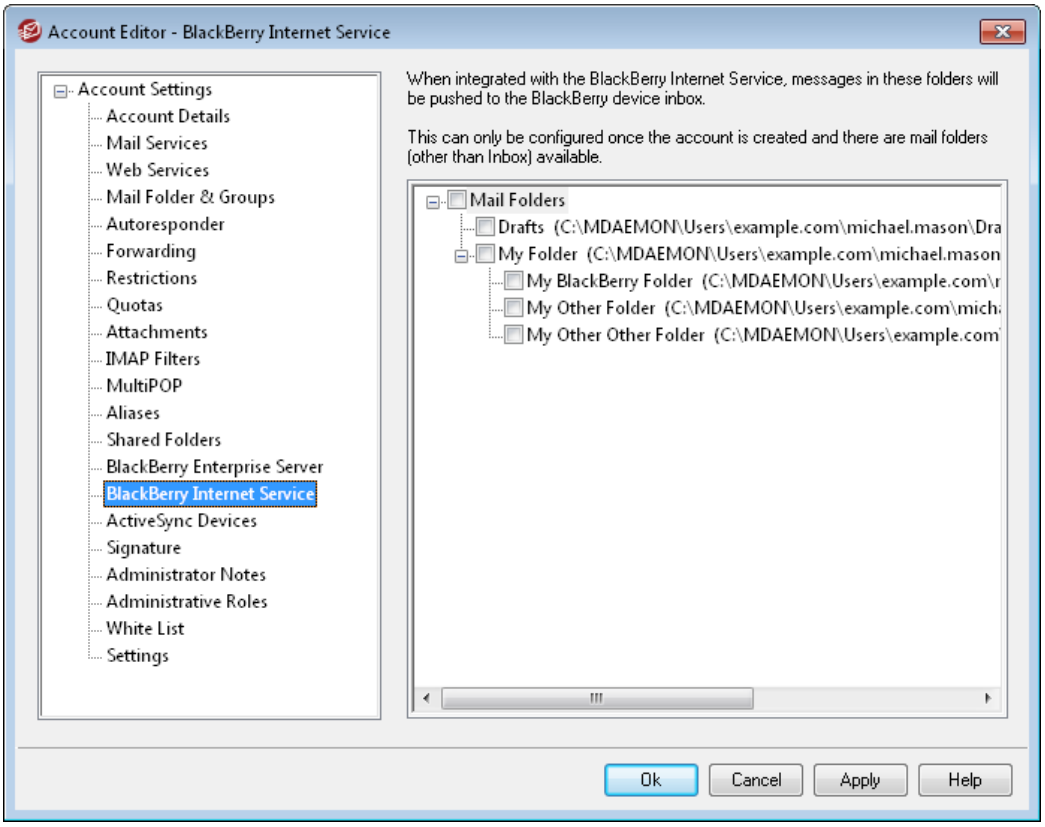
Erase work related data only
Click this button if you wish to erase only work related data from the BlackBerry device, such as when it is lost or stolen. This is only supported on BlackBerry devices running OS 6.0 MR2 or higher. The BlackBerry Enterprise Server's work-related data options are located under the BlackBerry Balance section of the Policies 319 screen. For more information, see: Deleting only work data from a device at blackberry.com.

See:

BlackBerry Enterprise Server 314

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.15 BlackBerry Internet Service



If a BlackBerry smartphone is using the BlackBerry Internet Service (BIS) to collect this account's email, you can use this screen to specify the IMAP folders whose new messages you wish to push to the smartphone's Inbox. Ordinarily the BlackBerry Internet Service only collects messages from the user's Inbox folder, not from any other folders associated with the user's account. Therefore if he or she is using IMAP filters 541 to sort messages automatically into specific folders, those messages will not be delivered to the BlackBerry device. This screen makes it possible for the user to get those filtered messages from whichever folders he or she chooses. This feature does not, however, deliver messages that were already contained in any of the folders—it only delivers new messages. If the account has no IMAP filters then this screen will be blank.

The folders themselves are not pushed to the BlackBerry device, only the new messages that are placed in them. All messages will be delivered to the device's Inbox, not to any specific folders on the device.

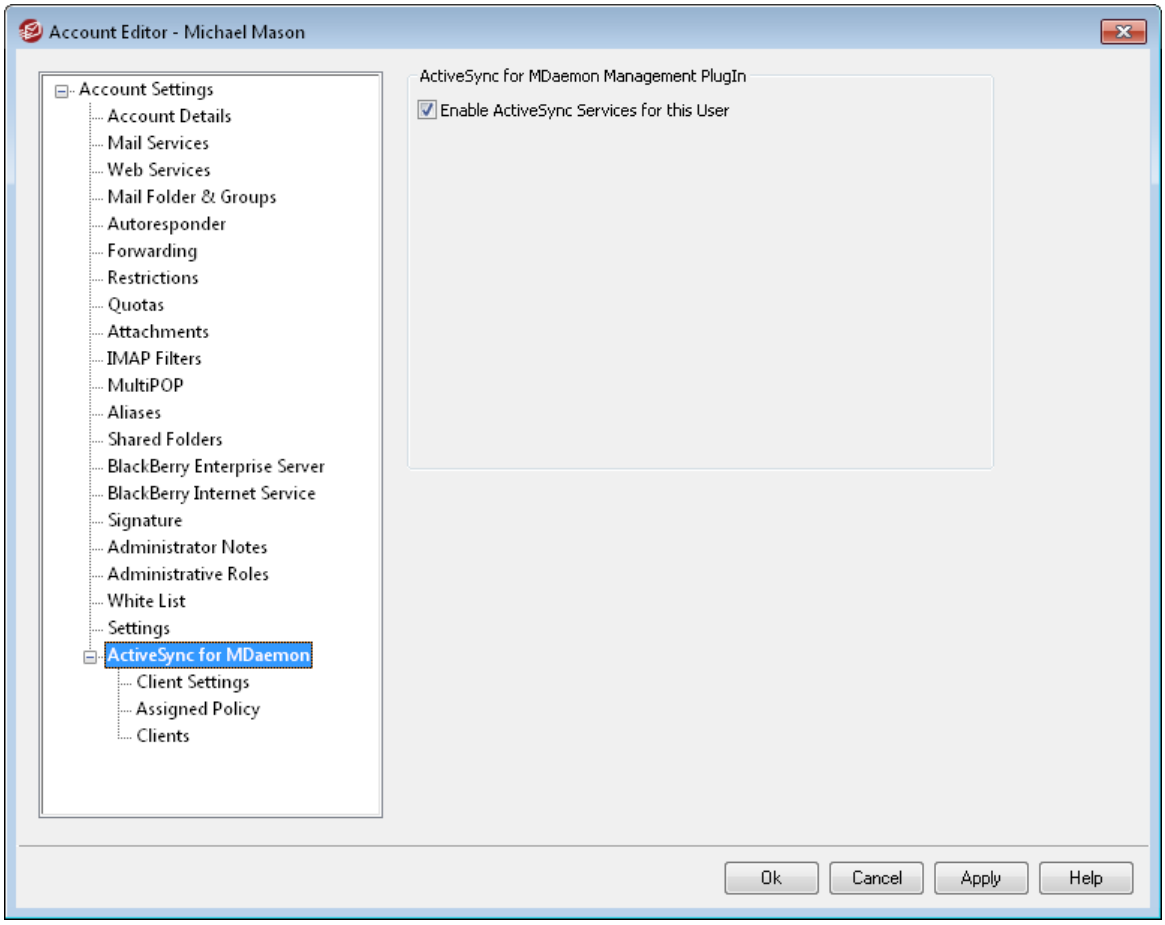
For users with access to WorldClient, the Folders page under Options in WorldClient contains this option so that users can manage the folder selection for themselves. This option, however, will only be available to them if the "*Allow selection of non-Inbox folder content to send to BlackBerry*" option on the BlackBerry Internet Service Settings 340 screen is enabled.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

BlackBerry » BlackBerry Internet Service 335

5.1.1.16 ActiveSync for MDaemon



The ActiveSync for MDaemon screens in the Account Editor are used to enable or disable ActiveSync for the account, configure account-specific settings 558, assign a default policy 561, and manage the account's ActiveSync clients 562.

Enabling/Disabling ActiveSync for the Account

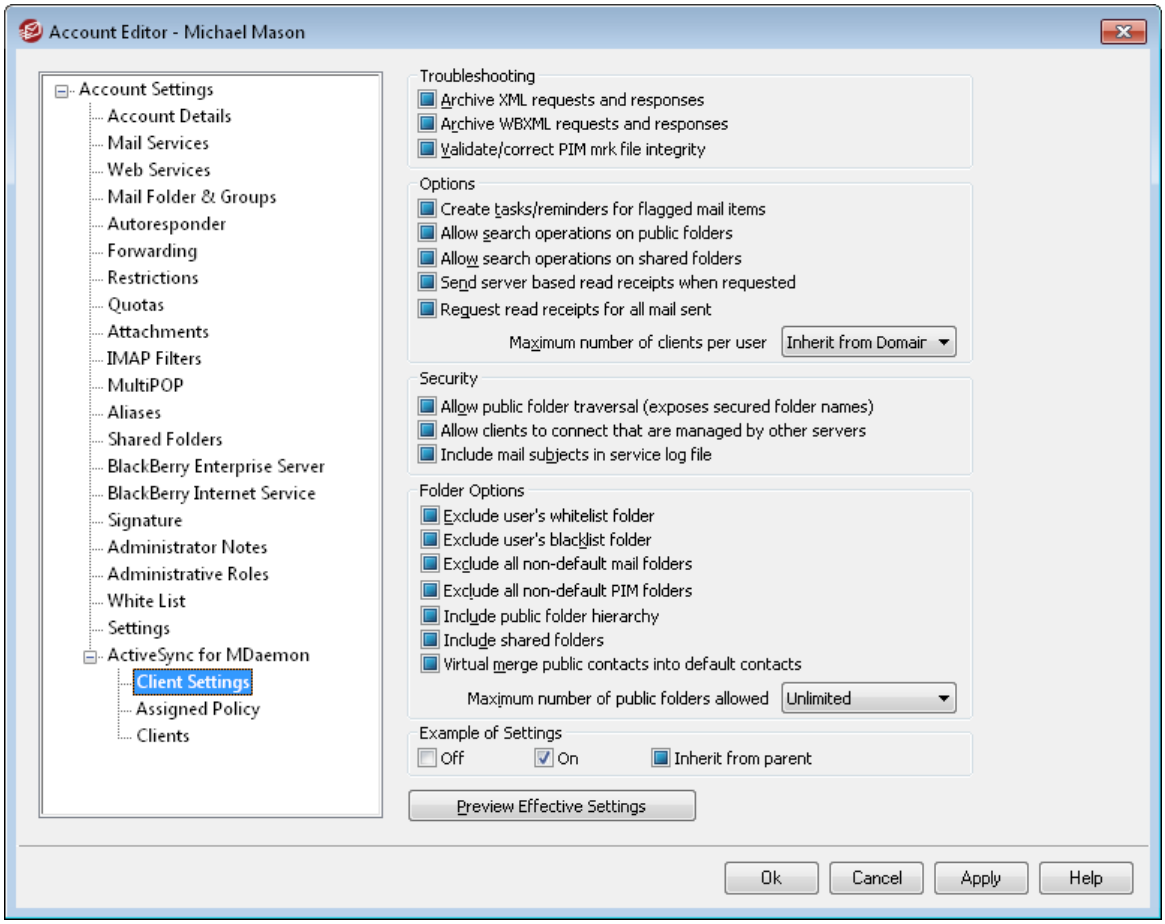
If you wish to allow the account to use an ActiveSync client to access its email and PIM data, enable this option.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Accout Editor » ActiveSync » Client Settings 558
Accout Editor » ActiveSync » Assigned Policy 561
Accout Editor » ActiveSync » Clients 562

5.1.1.16.1 Client Settings



The options on this screen are used to control ActiveSync client settings for clients associated with this account. By default each of these options is configured to inherit its setting from the corresponding domain to which the account belongs. Changing any setting on this screen will override the domain setting 292 for this account. Further, you can use the *Settings* option on the Clients 562 screen if you wish to override these account-level settings for specific clients.

Troubleshooting

Archive [XML | WBXML] requests and responses
Use the *Archive XML...* and *Archive WBXML...* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Options

Create Tasks/Reminders for flagged mail items
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email. This is disabled by default.

Allow search operations on Public Folders
Allows the client to search the Public Folders 218 to which it has access. This is allowed by default.

Allow search operations on Shared Folders
Allows the client to search the Shared Folders 547 to which it has access. This is allowed by default.

Send server based read receipts when requested.
Enable this option if you want the server to support read confirmation requests an issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Request read receipts for all mail sent
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Maximum number of clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default.

Security

Allow Public Folder traversal (exposes secured folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 220 for both the subfolder (i.e. child folder) and all parent public folders 218 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Allow clients to connect that are managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Disable this option if you do not wish to allows

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

those clients to connect.

Include mail subjects in service log file
Enable this option if you wish to include each message's Subject header in the ActiveSync log file. This is not recommended, and this option is disabled by default.

Folder Options

Exclude user's [whitelist/blacklist] folder
By default the user's whitelist and blacklist contact folders are not synced with devices. They are generally only used by MDaemon, to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Exclude all non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Exclude all non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include Public Folder hierarchy
Check this box if you want the public folders 218 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Include shared folders
Check this box if you want the shared folders 87 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Virtual merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Maximum number of Public Folders allowed
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 292, accounts 303, and clients 297). Since by default the options on those screens are set to

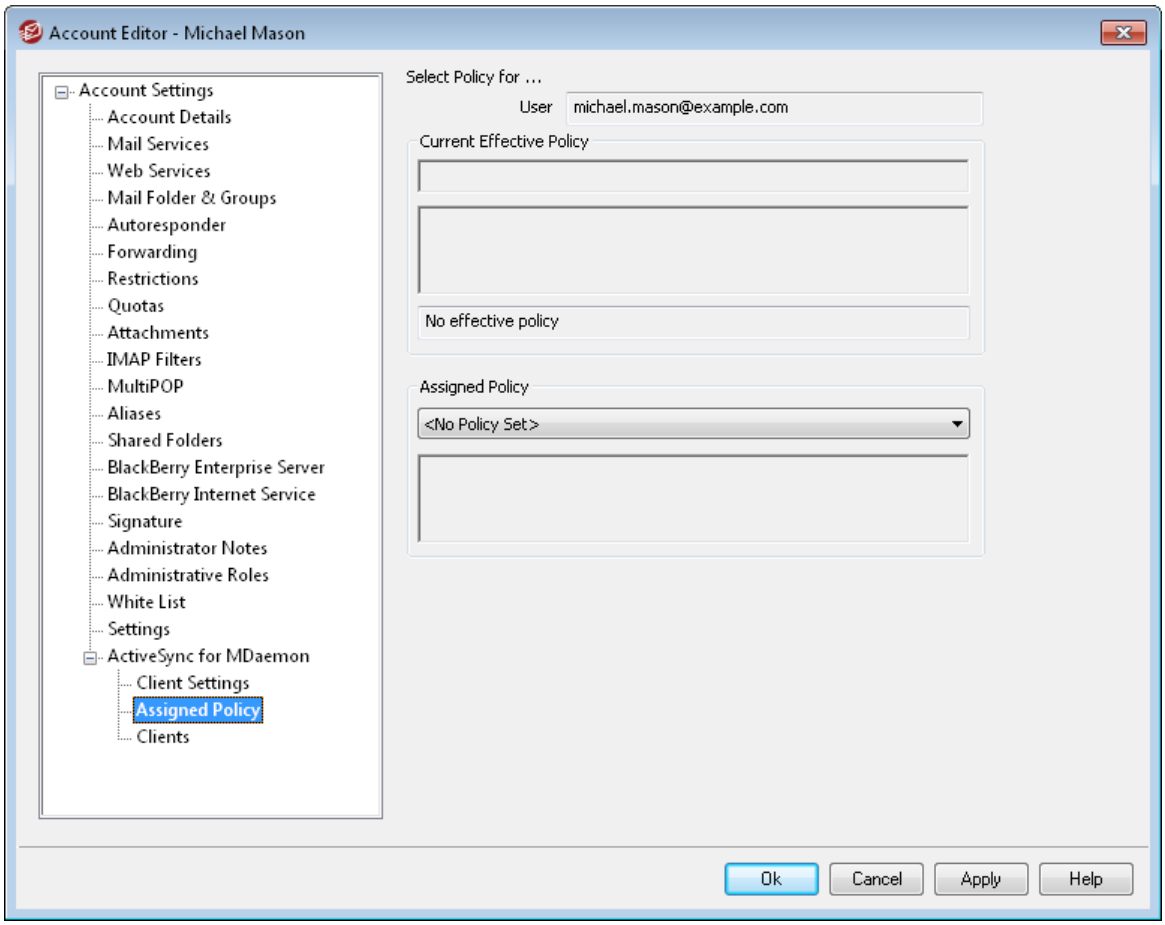
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Domains 292
Accout Editor » ActiveSync » Clients 562

5.1.1.16.2 Assigned Policy



Use this screen to designate the default ActiveSync Policy 284 that will be used for any ActiveSync client that connects using this account. By default this policy setting is inherited from the domain's policy 155 setting, but you can change it here to override that setting for this account. Further, you can also override this account-specific setting and assign a different policy to specific Clients 562.

Assigning an ActiveSync Policy

To assign a policy to the account, click the Assigned Policy drop-down list, choose the policy, and click **Ok** or **Apply**.

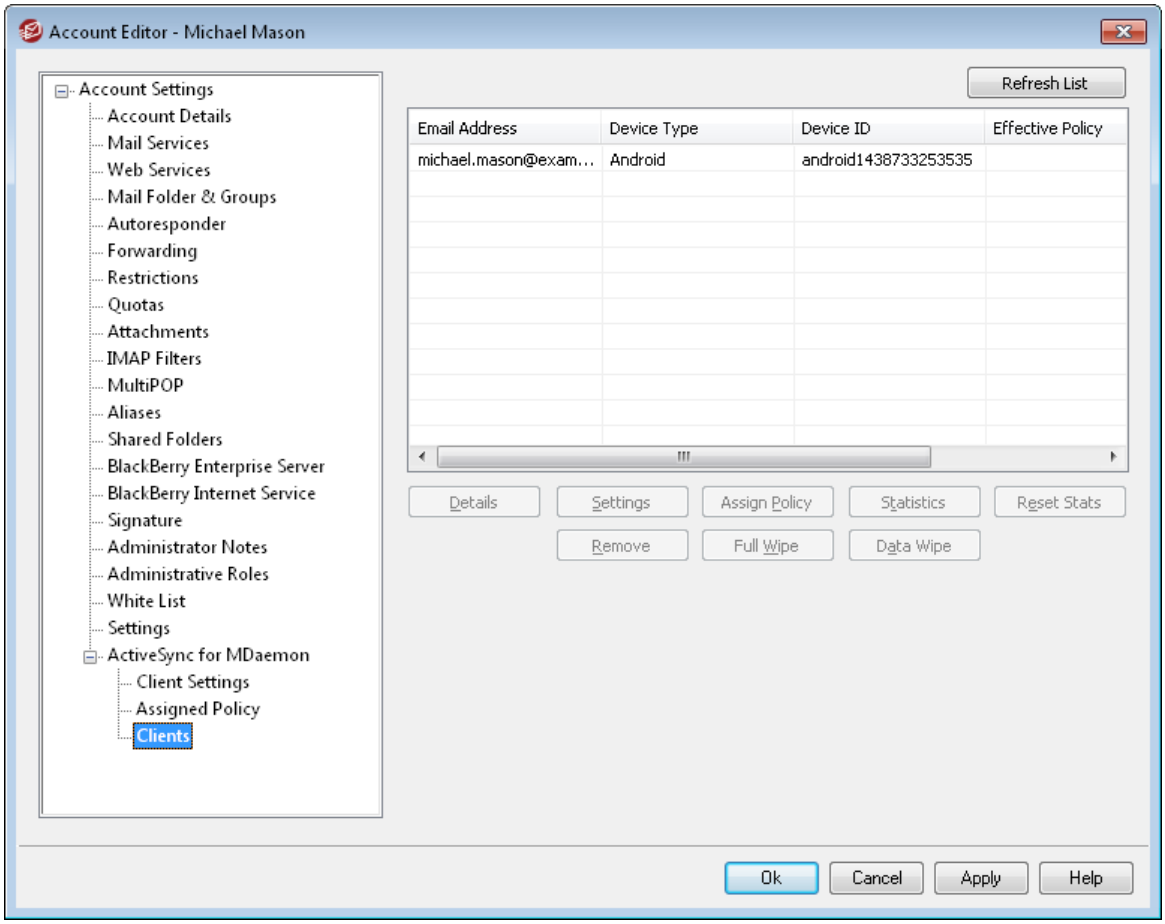
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Not all ActiveSync devices recognize or apply policies consistently. Some may ignore policies or certain policy elements altogether, and others may require a device reboot before changes take effect. Further, when attempting to assign a new policy, it will not be applied to a device until the next time the device connects on its own to the ActiveSync server; policies cannot be "pushed" to devices until they connect.

See:

ActiveSync » Policy Manager 284
ActiveSync » Domains 292
Accout Editor » ActiveSync » Clients 562

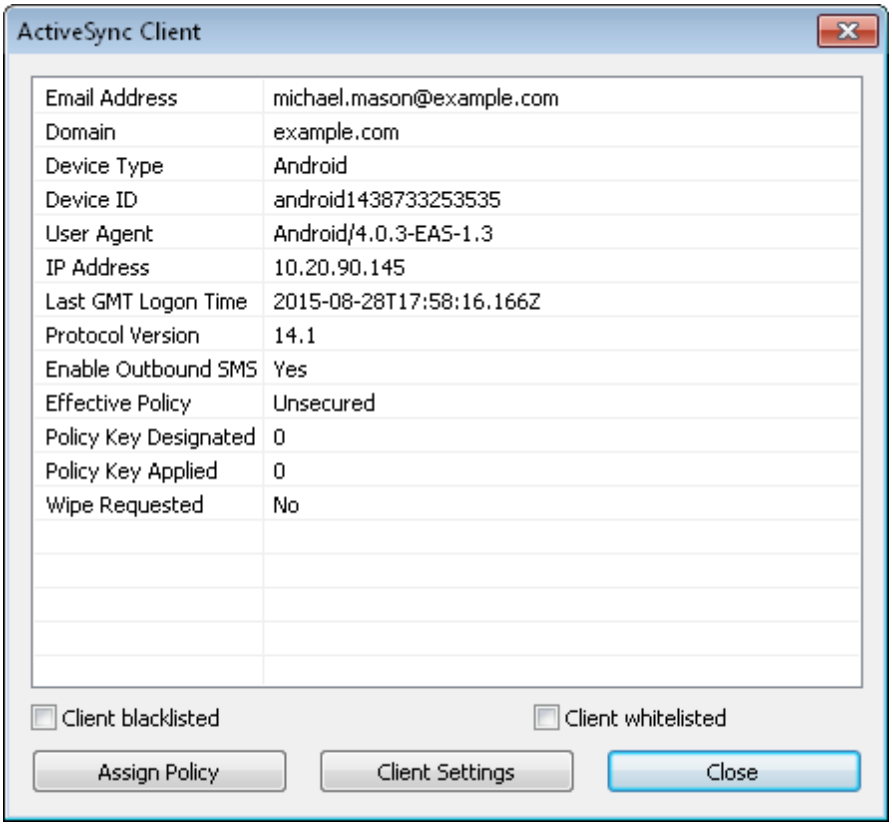
5.1.1.16.3 Clients



This screen displays information about any ActiveSync clients associated with the user's account. From here you can assign an ActiveSync Policy 561 for each client, control various client settings, remove clients, remotely wipe them, and reset the client statistics within MDaemon.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Details



Select an entry and click **Details** (or double-click the entry) to open the Client Details dialog. On this screen you can view information about the device, assign a policy, access its client settings, or add the device to the blacklist or whitelist 308.

Device Settings

Select a device and click **Settings** to manage the Client Settings for the device. By default these settings are inherited from the account's 303 Client Settings screen. See Managing a Device's Client Settings below.

Assigning an ActiveSync Policy

To assign a Policy 284 to the device:

1. Select a device from the list.
2. Click **Assign Policy**. This opens the Apply Policy dialog.
3. Click the Assigned Policy drop-down list and choose the desired policy.
4. Click **OK**.

Statistics

Click **Statistics** to open the Device Statistics dialog, containing various usage stats for the device.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Reset Stats

If you wish to reset the device's stats, click **Reset Stats**, and **Ok** to confirm the action.

Removing an ActiveSync Device

To remove an ActiveSync device, select the device and click *Remove*. This will remove the device from the list and delete all synchronization information related to it in MDaemon. Therefore if in the future the account uses ActiveSync to synchronize the same device, MDaemon will treat the device as if it had never before been used on the server; all device data will have to be re-synchronized with MDaemon.

Full Wiping an ActiveSync Device

To do a Full Wipe on an ActiveSync device, select the device from the list and click *Full Wipe*. The next time the device connects, MDaemon will tell it to erase all data, or restore itself to its factory default state. Depending on the device, this may remove everything on it, including downloaded apps. Further, as long as the device's ActiveSync entry exists in MDaemon, it will be wiped again if it ever connects again to MDaemon in the future. If you no longer wish to wipe the device when it connects (for example, if a lost device is recovered and you wish to use it again with the account) then you must first use the *Remove* option above to remove the device from MDaemon.

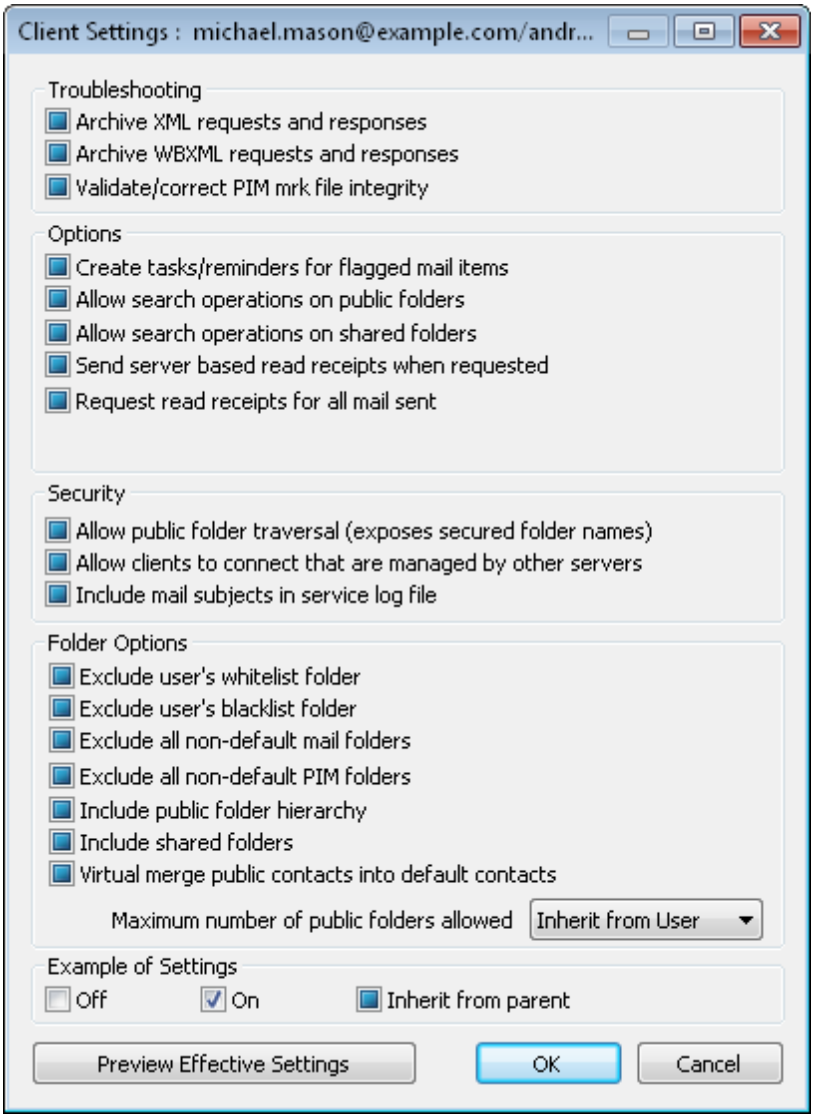
Data/Soft Wiping an ActiveSync Device

The *Data Wipe* (or *Soft Wipe*) option is similar to the *Full Wipe* option explained above, but instead of wiping all data, it will wipe only the account's data, such as its emails, calendar entries, contacts, and the like. The rest, such as apps, photos or music is left alone.

Managing a Device's Client Settings

The device-level Client Settings screen allows you to manage settings for a specific device.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.


Client Settings : michael.mason@example.com/andr...
Troubleshooting
Archive XML requests and responses
Archive WBXML requests and responses
Validate/correct PIM mrk file integrity
Options
Create tasks/reminders for flagged mail items
Allow search operations on public folders
Allow search operations on shared folders
Send server based read receipts when requested
Request read receipts for all mail sent
Security
Allow public folder traversal (exposes secured folder names)
Allow clients to connect that are managed by other servers
Include mail subjects in service log file
Folder Options
Exclude user's whitelist folder
Exclude user's blacklist folder
Exclude all non-default mail folders
Exclude all non-default PIM folders
Include public folder hierarchy
Include shared folders
Virtual merge public contacts into default contacts
Maximum number of public folders allowed
Inherit from User
Example of Settings
Off
On
Inherit from parent
Preview Effective Settings
OK
Cancel

By default all of the options on this screen are set to "Inherit from user," which means that each option will take its setting from the corresponding option on the account's Client Settings 303 screen. Any changes made to the settings on that screen will be reflected on this screen. Conversely, any changes you make to this screen will override the account-level setting for this device.

Troubleshooting

Archive [XML | WBXML] requests and responses
Use the *Archive XML...* and *Archive WBXML...* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

UIDs or empty required fields. The global option is disabled by default.

Options

Create Tasks/Reminders for flagged mail items
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email. This is disabled by default.

Allow search operations on Public Folders
Allows the client to search the Public Folders 218 to which it has access. This is allowed by default.

Allow search operations on Shared Folders
Allows the client to search the Shared Folders 547 to which it has access. This is allowed by default.

Send server based read receipts when requested.
Enable this option if you want the server to support read confirmation requests an issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Request read receipts for all mail sent
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Maximum number of clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default.

Security

Allow Public Folder traversal (exposes secured folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 220 for both the subfolder (i.e. child folder) and all parent public folders 218 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Allow clients to connect that are managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Disable this option if you do not wish to allows those clients to connect.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Include mail subjects in service log file
Enable this option if you wish to include each message's Subject header in the ActiveSync log file. This is not recommended, and this option is disabled by default.

Folder Options

Exclude user's [whitelist/blacklist] folder
By default the user's whitelist and blacklist contact folders are not synced with devices. They are generally only used by MDaemon, to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Exclude all non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Exclude all non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include Public Folder hierarchy
Check this box if you want the public folders 218 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Include shared folders
Check this box if you want the shared folders 87 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Virtual merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Maximum number of Public Folders allowed
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 292, accounts 303, and clients 297). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are

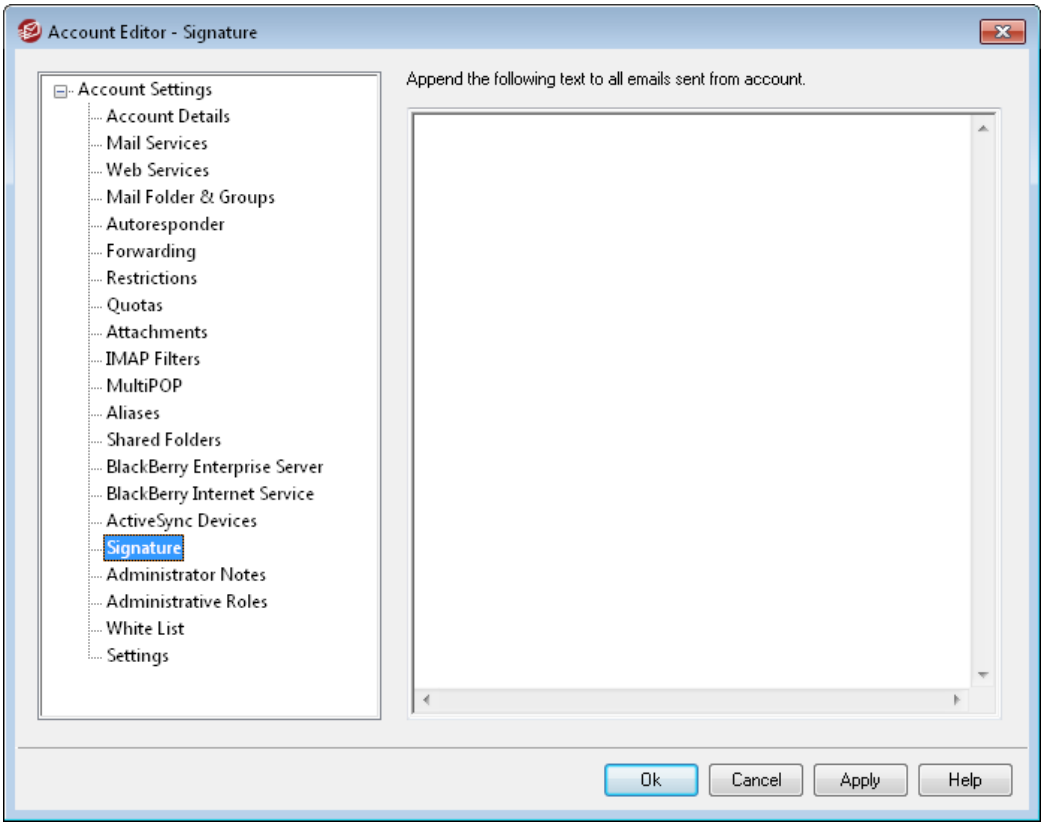
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

currently being applied to the displayed screen.

See:

ActiveSync » Client Settings 280
ActiveSync » Domains 292
ActiveSync » Accounts 303

5.1.1.17 Signature



Account Signature

Use this screen to designate a signature that will be appended to the bottom of every email that the account sends. This signature is added in addition to any other signatures or footers added by other options, such as the signature option included in WorldClient and other mail clients, the Default 83 and Domain 138 signature options, and Mailing List footers 206. Default/Domain Signatures and Mailing List footers are always added below Account Signatures.

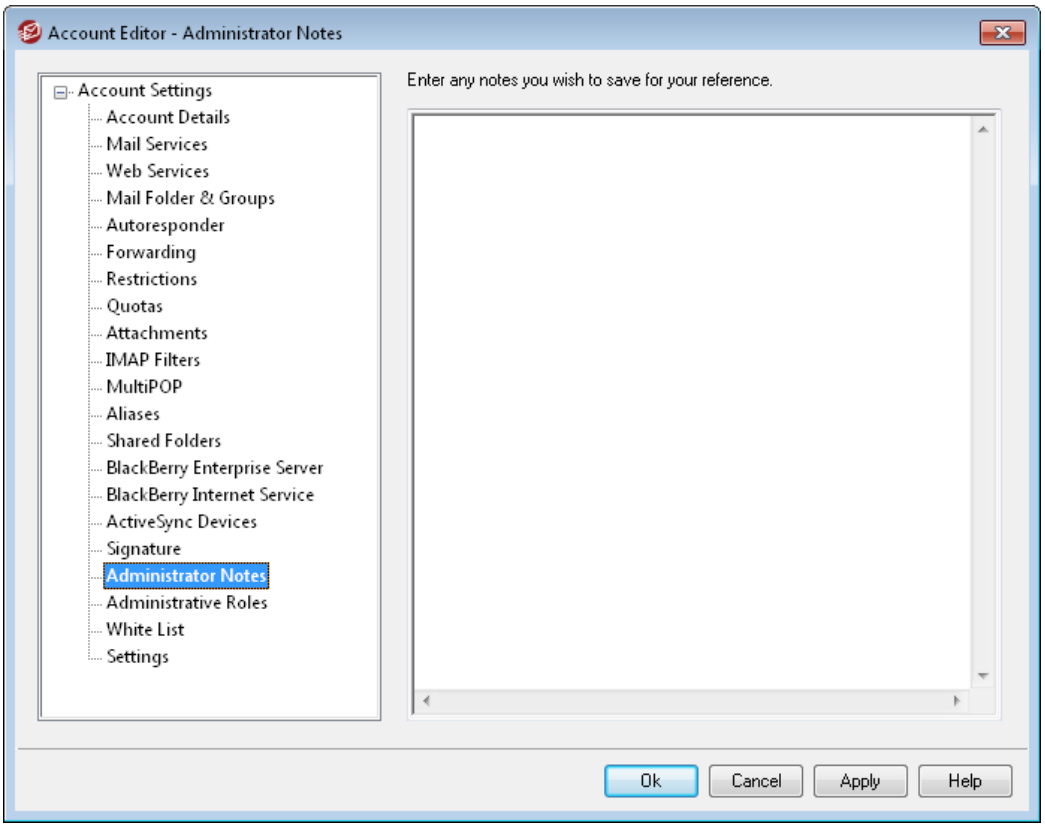
Users with access to WorldClient or Remote Administration 251 can edit their own signatures from there.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Default Signatures 83
Domain Signature 138
Mailing List Footers 206

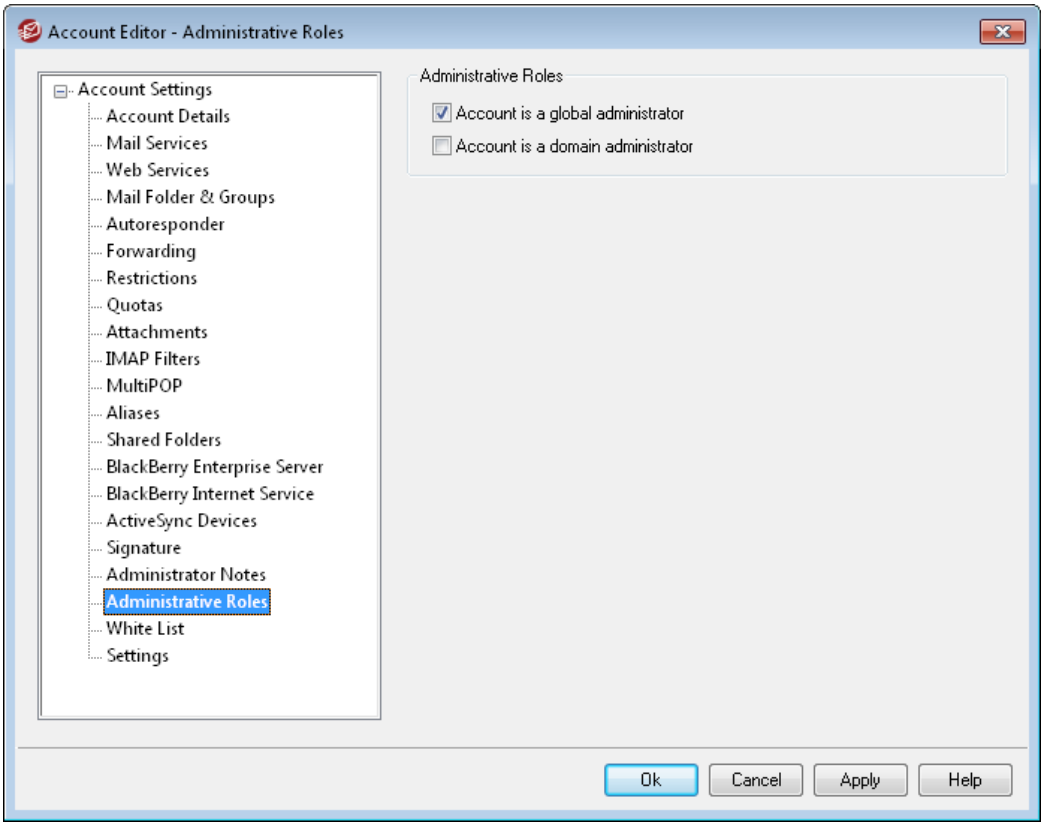
5.1.1.18 Administrator Notes



Use this screen for any notes or other information you wish to save for your own reference regarding this account. Unlike the *Description* field on the Account Details 521 screen, Administrator Notes will not be synchronized to the public contacts or mapped to any field in Active Directory.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.19 Administrative Roles



Administrative Roles

Account is a global administrator
Enable this checkbox to grant the user server-level administrative access. Global administrators have:

- Full access to server configuration, all users, and all domains via Remote Administration
- Access to all MDaemon users of all MDaemon domains as Instant Messaging buddies.
- The ability to post to all mailing lists even if flagged as "Read Only".
- The ability to post to all mailing lists even if not a member.

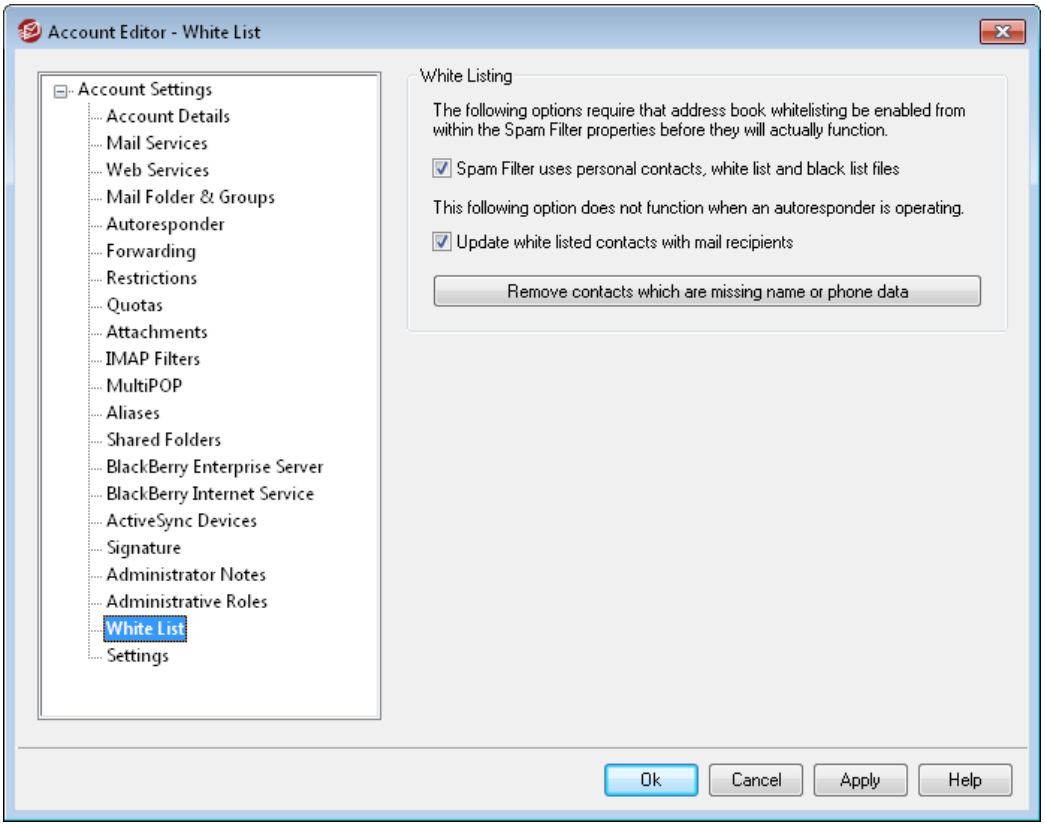
The user will have complete access to MDaemon's files and options. For more on the administrative options within the Remote Administration web-interface, see Remote Administration 251.

Account is a domain administrator
Click this checkbox to designate the user as a Domain Administrator. Domain administrators are similar to global administrators except that their administrative access is limited to this domain and to the permissions granted on the Web Services 526 page.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

If you wish to allow this account to administer a different domain, you can do so from within the Remote Administration 251 web interface, on the Domain Manager » Admins page.

5.1.1.20 White List



White Listing

Spam Filter uses personal contacts, white list, and black list files
The Spam Filter's White List (automatic) 413 screen contains a global option that can be used to cause the Spam Filter to white list a message automatically when the sender of the message is found in the local recipient's personal contacts or white list folder. It will also automatically black list a message when the sender is found in the user's black list file. If you have enabled the Spam Filter's global option but do not wish to apply it to this account, clear this check box to override the global setting. If the global option is disabled then this option will not be available.

Keeping your contacts updated and synchronized with WorldClient, the Windows Address Book, and other MAPI mail clients that use the Windows Address Book can be easily done using WorldClient Instant Messenger 227.

Update white listed contacts with mail recipients
Click this option if you wish to update this account's white list folder each time it

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

sends an outgoing message to a non-local email addresses. When used in conjunction with the above option, *Spam Filter uses personal contacts, white list, and black list files*, the number of Spam Filter false positives can be drastically reduced. The *Automatically update white listed contacts* option located on the White List (automatic) 413 screen must be enabled before you can use this feature.

This option is disabled when the account is using an autoresponder.

Remove contacts which are missing name or phone data
Click this button if you wish to remove every contact that contains only an email address from the account's default Contacts folder. If a contact doesn't have at least a name or phone data it will be removed. The option is primarily to help those who were using MDaemon's automatic white listing option prior to version 11 purge contacts that were added purely as a function of the white list feature. In previous versions of MDaemon the addresses were added to the main contacts instead of to a dedicated white list folder. This could result in the account having many entries in the contacts folder that the user would rather not have there.

Consider this option carefully before using it, because contacts containing only an email address could still be legitimate.

Setting the Default Values for New Accounts and Groups

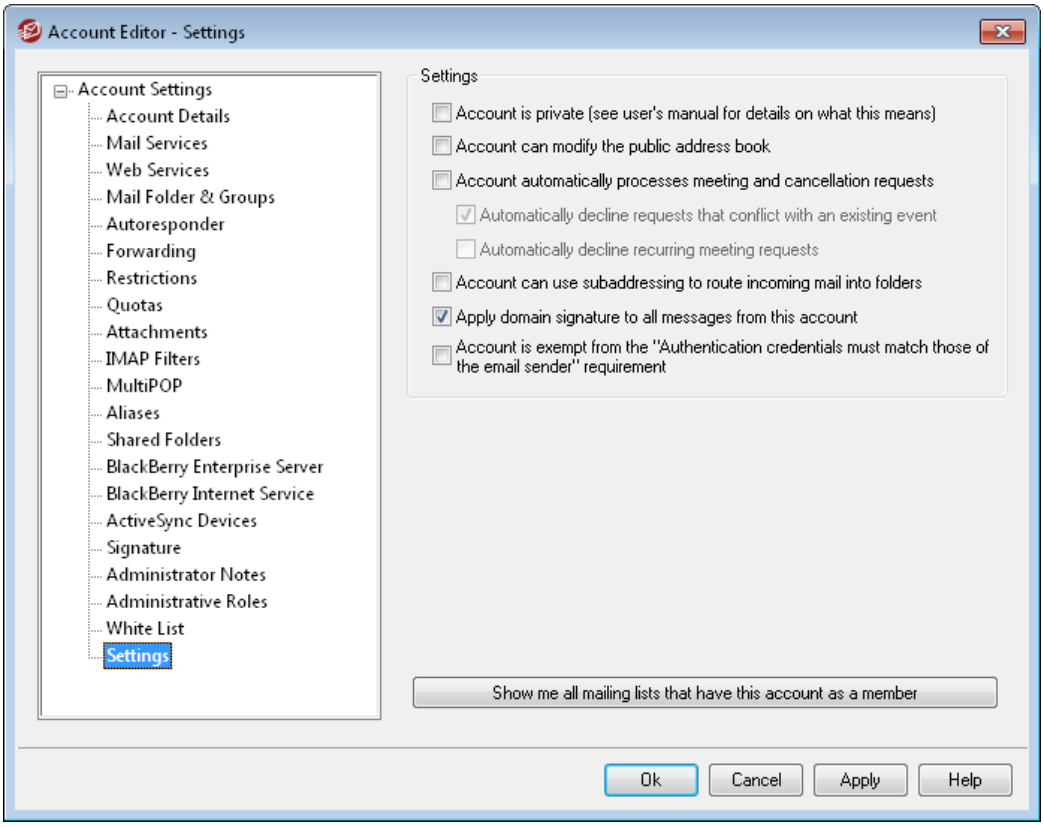
The options on this screen correspond to those located on the Template Properties » White List 602 screen, which can be used to set the default values for new accounts 581 and values for accounts belonging to certain groups 576.

See:

White List (automatic) 413
Template Manager 580
Template Properties » White List 602

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.1.1.21 Settings



Settings

Account is private
MDaemon can automatically create and maintain "Everyone@" and "MasterEveryone@" mailing lists 183, which can be used to send a message to all of a domain's users and all MDaemon users, respectively. By default these lists include all accounts of each domain, but you can check this box if you wish to exclude this account from those lists. This will also hide the account from shared calendars and VRFY 53 results. The account's address book entry, however, will not be hidden from a global address book lookup performed on a BlackBerry device that is activated on your MDaemon's BlackBerry Enterprise Server.

Account can modify the public address book
Click this option if you want the account to be able to add and delete entries from the WorldClient or LDAP-based public address books.

> If the Account is synchronizing folders with WorldClient Instant Messenger 227 then modifications could be propagated to all users. Exercise caution when enabling this feature.

Account automatically processes meeting and cancellation requests
Click this checkbox if you wish to cause automatic processing of meeting requests,

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

changes, and cancellations for this account. When the account receives a message that contains a meeting request, the account's calendar will be updated automatically. This option is disabled for all accounts by default.

Automatically decline requests that conflict with an existing event
If automatic processing of meeting requests and cancellations is enabled for this account, those meeting requests will be automatically declined by default when they conflict with an existing event. Clear this checkbox if you wish to allow the conflicting event to be created.

Automatically decline recurring meeting requests
Click this box if automatic processing of meeting requests and cancellations is enabled for this account but you wish to decline those requests when they are for recurring meetings.

Account can use subaddressing to route incoming mail into folders
Click this checkbox if you wish to permit subaddressing 574 for this account.

Apply domain signature to all messages from this account
When there is a Domain Signature 138 for the domain to which this account belongs, this option causes it to be added to all emails sent by the account. It is enabled by default.

Account is exempt from the "Authentication credentials must match those of the email sender" requirement
Use this option if you wish to exempt the account from the "*Authentication credentials must match those of the email sender*" global option located on the SMTP Authentication 442 screen. This option is disabled by default.

Show me all mailing lists that have this account as a member
Click this button to open a list of all Mailing Lists 180 that have this account as a member.

Subaddressing

Subaddressing is a system for including a folder name in the mailbox portion of an account's email address. Using this system, messages addressed to the *mailbox +folder* name combination will be routed automatically to the account's folder included in the address (assuming that folder actually exists), without the need to create specific filtering rules to make that happen.

For example, if `bill.farmer@example.com` has an IMAP mail folder called "`stuff`," then mail arriving addressed to "`bill.farmer+stuff@example.com`" would be routed automatically to that folder. Subfolders can be designated by including the folder and subfolder names separated by an additional "+" character, and underscores are used to replace spaces in folder names. So, using the example above, if Bill's "`stuff`" folder had a subfolder called "`my older stuff`," then messages addressed to "`bill.farmer+stuff+my_older_stuff@example.com`" would be routed automatically to Bill's "`\stuff\my older stuff\`" mail folder.

Since subaddressing requires the use of the "+" character, mailboxes that contain "+"

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

cannot be subaddressed. So, in the example above, if the actual address were "bill+farmer@example.com" instead of "bill.farmer@example.com" then it could not be subaddressed. Further, you cannot use an address alias in a subaddress. You can, however, create an alias that refers to an entire subaddressed form. So, even though "alias+stuff@example.com" is not permitted, using "alias@example.com" to point to "bill.farmer+stuff@example.com" would be fine.

To prevent exploits or abuse, the IMAP folder included in the subaddress **must** be valid. If a subaddressed message arrives for an account that does not have a folder matching the name of the folder defined in the subaddress, then the subaddress will be treated as an unknown email address and handled accordingly, based on your other MDaemon settings. For example, if bill.farmer@example.com does not have a folder named "stuff" and yet a message arrives for "bill.farmer+stuff@example.com" then that message will be treated as if were addressed to an unknown user, and it will most likely be rejected.

By default, each account has the subaddressing feature disabled. You can, however, disable this feature globally via the *Disable subaddressing feature for all accounts* option located on the Miscellaneous 354 screen of the Preferences dialog. If Subaddressing is disabled via that option, it will not be permitted for any account, regardless of the individual account settings.

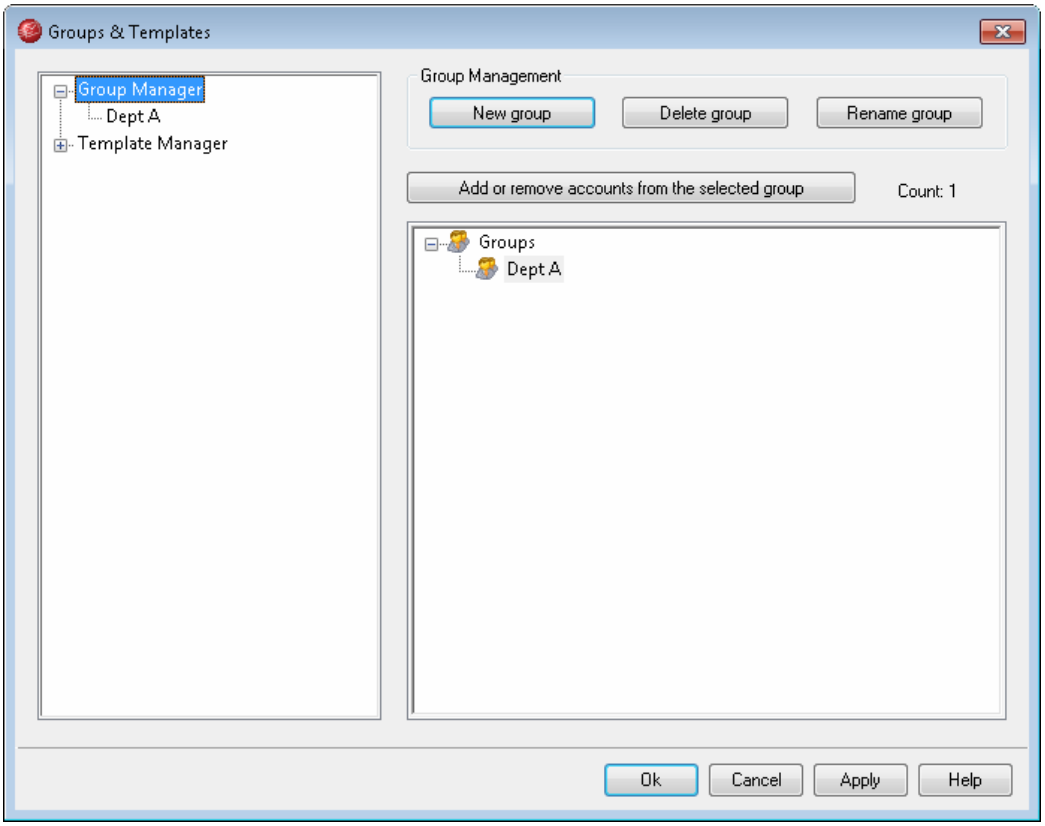
See:

White List (automatic) 413
Remote Administration 251
Template Manager 580

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.2 Groups & Templates

5.2.1 Group Manager



The Group Manager (Accounts » Groups & Templates... » Group Manager) is used to create account Groups and manage which accounts belong to them. Groups have a number of different uses and functions. For example, using the Group Properties 577 screen you can assign an account template 580 to a Group, allowing you to control a variety of account settings for group members. You can also control whether or not group members have access to WorldClient Instant Messenger 225 and instant messaging. Further, the Content Filter supports groups, allowing you to create rule conditions 366 based on whether or not a message sender or recipient is a member of a specific Group. Finally, for Shared Folders 84 you can assign Access Control List 220 rights to specific Groups, meaning all members of that Group will share those access rights.

You can add accounts to a Group by selecting the Group from the list below and then clicking the "*Add or remove accounts...*" button. You can also add users to Groups from each user's Mail Folder & Groups 524 screen.

Group Management

New group
To create a new Account Group, click *New group*, type a name and description for the group, and click *OK*. The new group will appear in the list of groups below and in the left pane.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Delete group
To delete a group, select the group in the list below, click *Delete group*, and click *Yes* to confirm your decision to delete the group.

Rename group
To rename a group, select the group in the list below and click *Rename group*. Type a new name for the group and click *OK*.

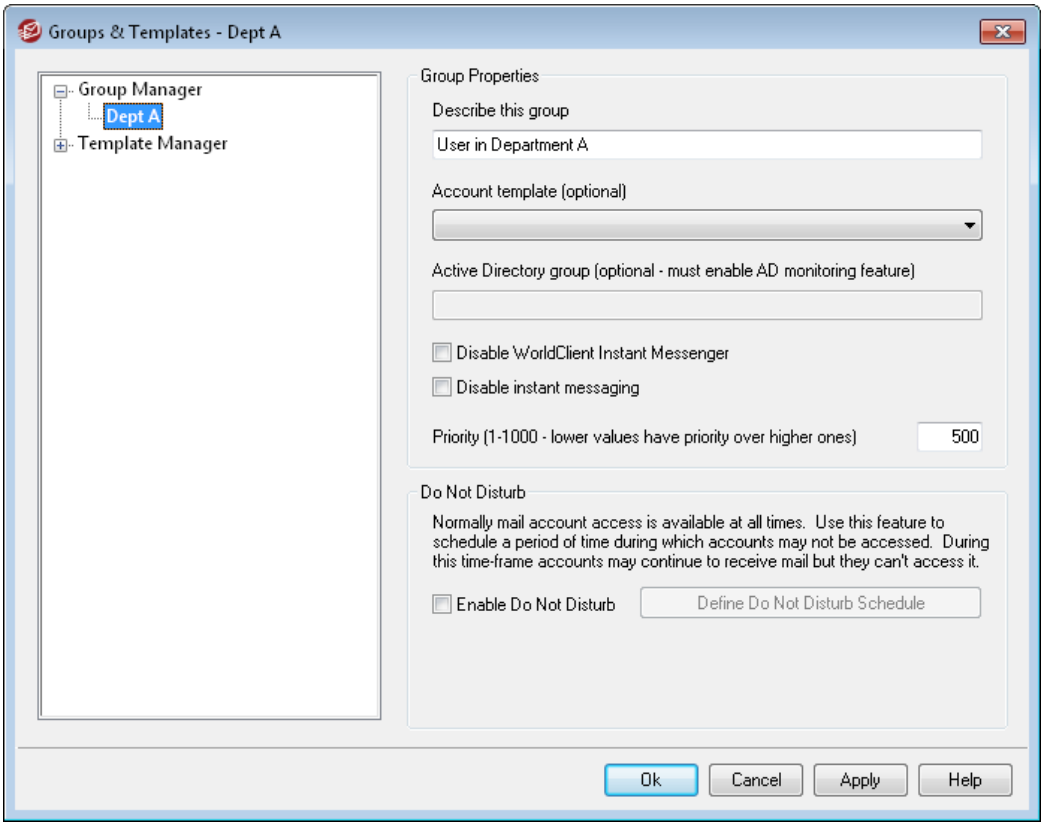
Add or remove accounts from the selected group

To manage a group's membership, select a group from the list below and click this button. Click the checkbox next to any accounts you wish to add to the group and clear the checkbox next to any members you wish to remove. Click *Ok*.

See:

Mail Folder & Groups 524
Creating a New Content Filter Rule 366
Shared Folders 84

5.2.1.1 Group Properties


Groups & Templates - Dept A
Group Manager
Dept A
Template Manager
Group Properties
Describe this group
User in Department A
Account template (optional)
Active Directory group (optional - must enable AD monitoring feature)
Disable WorldClient Instant Messenger
Disable instant messaging
Priority (1-1000 - lower values have priority over higher ones)
500
Do Not Disturb
Normally mail account access is available at all times. Use this feature to schedule a period of time during which accounts may not be accessed. During this time-frame accounts may continue to receive mail but they can't access it.
Enable Do Not Disturb
Define Do Not Disturb Schedule
Ok
Cancel
Apply
Help

The Group Properties screen (Accounts » Groups & Templates... » [group name]) is used to configure the settings for each group you have created using the Group

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Manager[576]. To open Group Properties from the Group Manager, double-click the group you wish to edit, or click the name of the group in the left pane. On this screen you can assign an Account Template[580] to a group, allowing you to control a variety of account settings for group members. You can also link the group to an Active Directory group, control whether or not group members have access to WorldClient Instant Messenger (WCIM)[225] and instant messaging, and set a priority level for the group. To control group membership, use the Group Manager and Mail Folder & Groups[524] screen on the Account Editor.

Group Properties

Describe this group
Enter a description of the group here, for your own reference. This information is typically entered when you create the group but can be edited from this screen at any time.

Account template (optional)
If you have created an Account Template[580] that you would like to use to control some of the account settings for group members, use this drop-down list to select the desired template. When an account template is linked to a group, any category of account settings designated on Template Properties[582] will be used for all accounts belonging to the group. The template will be used to control those settings rather than using the individual account settings on the Account Editor. If an account is removed from a group that was controlling its account settings, the settings will revert to the values designated by the New Accounts template[581].

Active Directory group (optional - requires AD monitoring)
Use this option if you wish to link the group to a specific Active Directory group. Members of the Active Directory group will added to the account group automatically. But for this to work you must be using the Active Directory Monitoring[608] feature.

You can map any Active Directory attribute you want to use as a trigger for adding accounts to Groups, although the "`memberOf`" attribute will most likely be the one to use. You can configure this by editing `ActiveDS.dat` in notepad. This feature is disabled by default. To enable it, edit `ActiveDS.dat` and specify which attribute to use for your group trigger, or uncomment the "`Groups=%memberOf%`" line in `ActiveDS.dat` to use it.

Disable WorldClient Instant Messenger
Click this box if you wish to disable WCIM support for all members of the group.

Disable Instant Messaging
Click this box if you wish to allow support for WCIM but not its Instant Messaging feature.

Priority (1-1000 - lower values have priority over higher ones)
Use this option to set a priority level (1-1000) for your groups, which allows accounts to be members of multiple groups and avoid possible conflicts between group settings. For example, when an account is a member of multiple groups that each have a linked account template controlling the same settings, the settings for

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

the group with the first Priority will be used. In other words, a group with a Priority value of "1" will be over a group with a value of "10". When there is no conflict the settings for each group are collectively applied. In the case of a tie the first group found wins. When an account is removed from a group linked an account template, the account settings previously controlled by the account template will change to the account settings designated by the next Priority group. If there isn't another group controlling those settings, then they will revert to settings designated by the New Accounts template 581.

Do Not Disturb

Use the Do Not Disturb feature to schedule a time frame during which an account may not send mail or be accessed by its users. Access during a Do Not Disturb period is not allowed and returns an appropriate error response to IMAP, POP, SMTP, ActiveSync, and WorldClient access requests. MDaemon will still accept incoming mail for accounts in this state, but those accounts may not send mail or be accessed by mail clients.

To apply Do Not Disturb to one or more accounts:

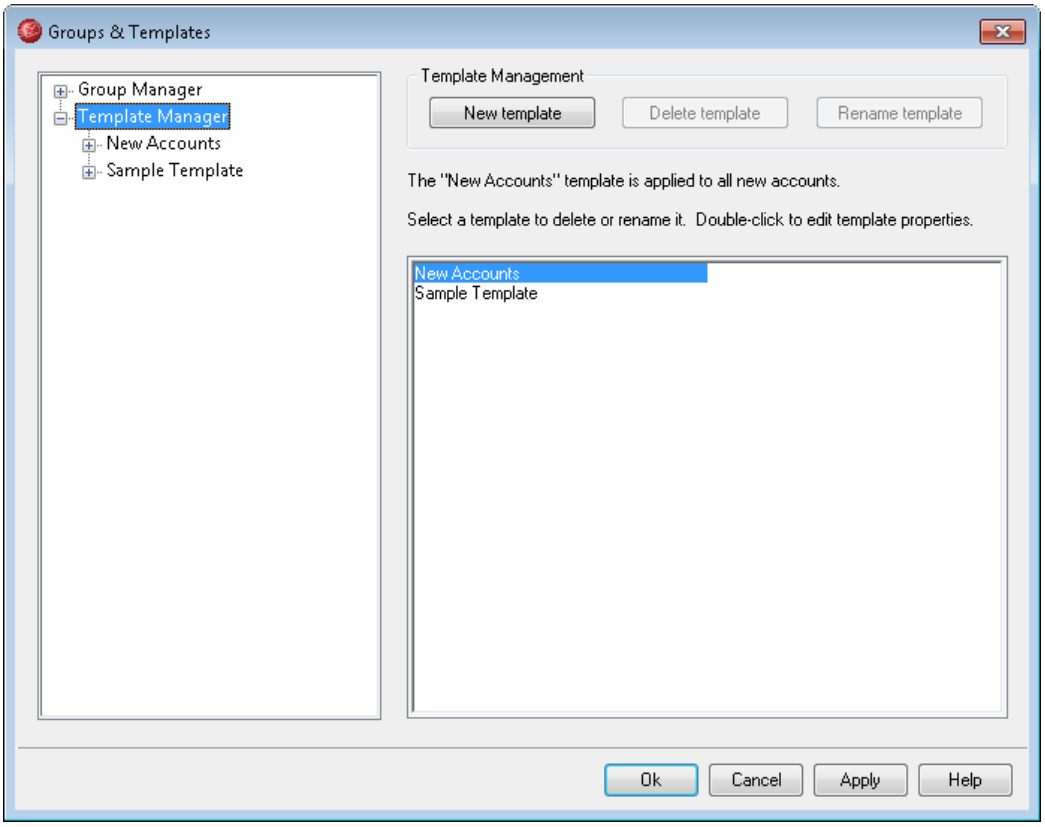
1. Click **Enable Do Not Disturb**.
2. Click **Define Do Not Disturb Schedule**.
3. Set the start/end dates, the start/end times, and the days of the week to use it.
4. Click **Ok**.
5. Use the Group Manager 576 to assign any accounts to this group that you wish to use it.

See:

Group Manager 576
Mail Folder & Groups 524
Template Manager 580
Template Properties 582

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.2.2 Template Manager



With the Template Manager (Accounts » Groups & Templates... » Template Manager) you can create and manage Account Templates, which are named sets of account settings that can be assigned to specific Groups 576. Any account belonging to one or more of those groups will have the designated account settings locked, being controlled only by the assigned templates rather than by the Account Editor. The categories of account settings that a template will control are designated on each template's properties 582 screen, which is reached by double-clicking the template's name in the list below, or by clicking the template in the left pane.

Template Management

New template

To create a new Account Template, click *New template*, type a name for the template, and click *OK*. The new template will appear in the list of templates below and in the left pane.

Delete template

To delete a template, select the template in the list below, click *Delete template*, and click *Yes* to confirm your decision to delete the template.

Rename template

To rename a template, select the template in the list below and click *Rename template*. Type a new name for the template and click *OK*.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Template List

The list on the bottom of the Template Manager contains all your templates. Click a template and then use the buttons at the top of the screen to delete or rename it. Double-click a template to open its properties 582 screen from which you can designate the categories of account settings that it will control. You can jump directly to any template and its account settings using the controls in the left pane. The *New Accounts* template is a special template that always appears first in the list.

New Accounts Template

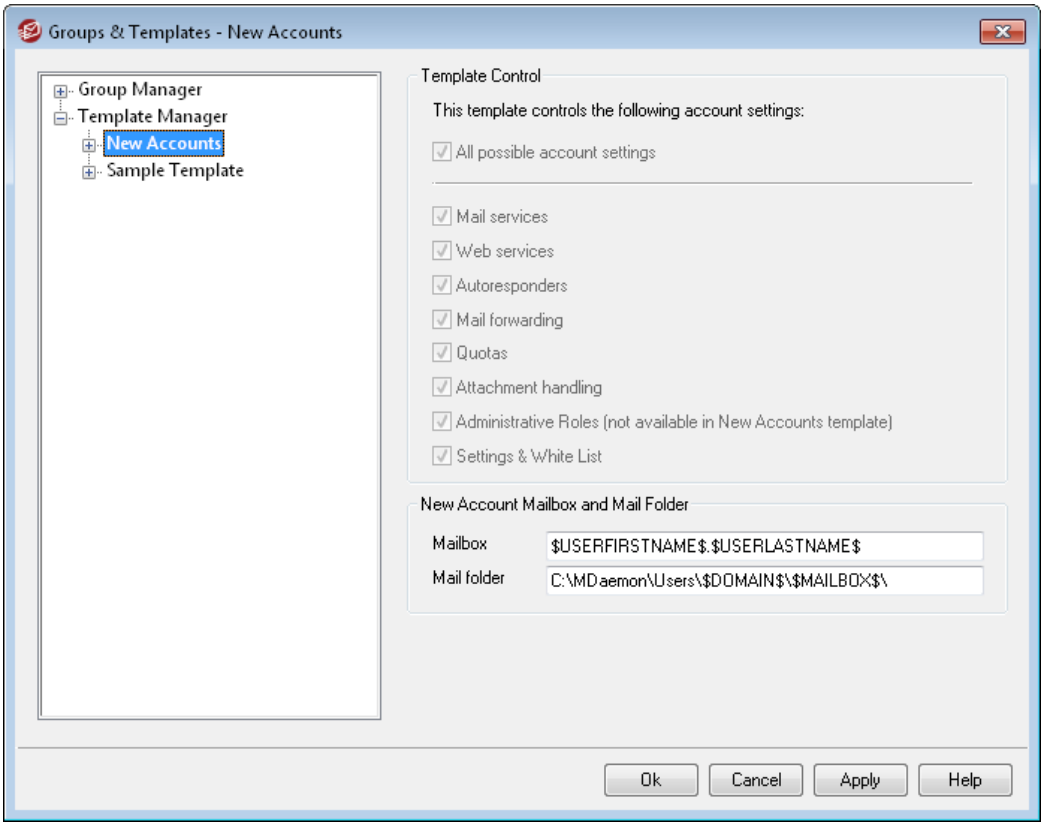
The *New Accounts* template is a special template that is applied to all new accounts when they are created. Rather than locking and controlling certain account settings like other templates, *New Accounts* is used simply to designate the initial settings for new accounts. Those initial settings can then be changed normally by using the Account Editor to edit individual accounts. Some template settings, such as the options located on the Administrative Roles 601 screen, are not available to the New Accounts template.

See:

Template Properties 582
Group Manager 576

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.2.2.1 Template Properties



To access a template's properties screen, open the Template Manager[580] and click the template's name in the left pane. Use each template's properties screen to designate the categories of account settings that the template will control. Any account belonging to a Group[576] that utilizes an account template will have the corresponding Account Editor screens locked, since those settings will be controlled by the template.

Template Control

All possible account settings
Click this checkbox if you would like this template to control all available account settings for Groups[576] using the template. All of the template screens will be used for each group member's account settings instead of the corresponding screens of the same name on the Account Editor. Clear this check box if you wish to use the *Account Settings* options below to pick specific account settings to control.

Account Settings
This section lists all of the categories of account settings that the template may control for Groups utilizing the template. Each option corresponds to the template screen of the same name. When an option is selected, the settings on that template screen will be used instead of the settings on the corresponding Account Editor screen for associated group members.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

New Account Mailbox and Mail Folder

These options are only available on the New Accounts template 581. They use a variety of special macros 583 to automatically generate the mail storage folder and the mailbox portion of the email address for new accounts.

Mailbox
Use this field to control the default *Mailbox name* 521 portion of the email address that will be generated for new accounts. See Template Macros 583 below for a list of the Macros that can be used in this template string.
"$USERFIRSTNAME$.$USERLASTNAME$" is the default template for this option. Therefore creating an account for "Michael Mason" under the example.com domain would result in his address being set to "Michael.Mason@example.com".

Mail folder
Use this field to control the default *Mail folder* 524 that will be used for new accounts. Each account's *Mail folder* is where its email messages will be stored on the server. For example, "...\$DOMAIN$\$MAILBOX$\" would create the path, "...\example.com\michael.mason\" for the user, "michael.mason@example.com".

MDaemon supports a basic system for folder hashing. Under NTFS, keeping many folders under the same root can sometimes cause performance problems. If you have large numbers of users and wish to subdivide the user folders beyond the default $DOMAIN$\$MAILBOX$\ setup, you can use the macro $MAILBOXFIRSTCHARSn$ to do so. Using this macro, "n" is a number between 1 and 10 and will expand to the first "n" characters of the mailbox name. Changing your default *Mail folder* path to something like the following will achieve a decent folder hashing system:

```
C:\MailboxRoot
\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCHARS2$\$MAILBOX$
\.
```

Template Macros

Below is a quick reference to the macros available for automating your account setup.

$DOMAIN$	This variable will resolve to the domain name selected for the account.
$DOMAINIP$	This variable will resolve to the IPv4 address associated with the domain currently selected for the account.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

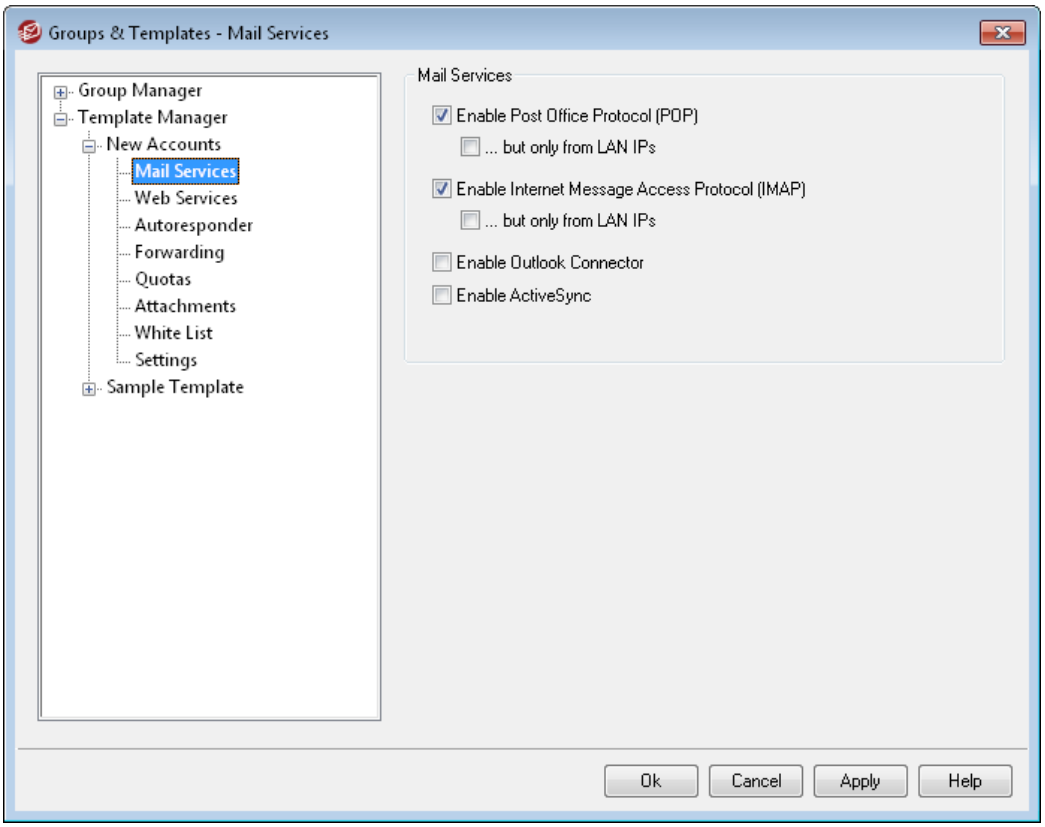
$DOMAINIP6$	This variable will resolve to the IPv6 address associated with the domain currently selected for the account.
$MACHINENAME$	This macro returns the host name of the Default Domain, from the Host Name & IP screen of the Domain Manager. The macro is now used in the default account information script (NEWUSERHELP.DAT) for new installations.
$USERNAME$	This variable resolves to the full first and last name of the account holder. This field is equivalent to "$USERFIRSTNAME$ $USERLASTNAME$"
$USERFIRSTNAME$	This variable resolves to the first name of the account holder.
$USERFIRSTNAMELC$	This variable resolves to the first name of the account holder, in lower case letters.
$USERLASTNAME$	This variable resolves to the last name of the account holder.
$USERLASTNAMELC$	This variable resolves to the last name of the account holder, in lower case letters.
$USERFIRSTINITIAL$	This variable resolves to the first letter of the account holder's first name.
$USERFIRSTINITIALLC$	This variable resolves to the first letter of the account holder's first name, in lower case.
$USERLASTINITIAL$	This variable resolves to the first letter of the account holder's last name.
$USERLASTINITIALLC$	This variable resolves to the first letter of the account holder's last name, in lower case.
$MAILBOX$	This variable resolves to the mailbox name of the current account. The value will also be used as the value of the USER command passed during POP3 mail sessions.
$MAILBOXFIRSTCHARSn$	Where "n" is a number between 1 and 10. This will expand to the first "n" characters of the mailbox name.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Template Manager 580
Group Manager 576

5.2.2.1.1 Mail Services



The options on this template screen correspond to the options located on the Account Editor's Mail Services 525 screen. When a template is set to control this screen 582, it will control the Mail Services options for any account belonging to a Group 577 that utilizes the template.

Mail Services

Enable Post Office Protocol (POP)
When this box is checked, accounts with settings controlled by this template can be accessed via Post Office Protocol (POP). Virtually all email client software supports this protocol. Clear this checkbox if you do not wish to allow POP access.

...but only from LAN IPs
Check this box if you wish to allow accounts to be accessed via POP only when the user is connecting from a LAN IP address 514.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Enable Internet Message Access Protocol (IMAP)
When this box is checked, accounts with settings controlled by this template can be accessed via Internet Message Access Protocol (IMAP). IMAP is more versatile than POP, allowing email to be managed on the server and accessed using multiple clients. Most email client software supports this protocol. MDaemon Pro is required for IMAP support.

...but only from LAN IPs
Check this box if you wish to allow accounts to be accessed via IMAP only when the user is connecting from a LAN IP address 514.

Enable Outlook Connector
This option is only available on the New Accounts template. Click this checkbox if you wish to allow new accounts to share Microsoft Outlook folders using Outlook Connector for MDaemon 625. **Note:** this option will only be available when Outlook Connector is installed.

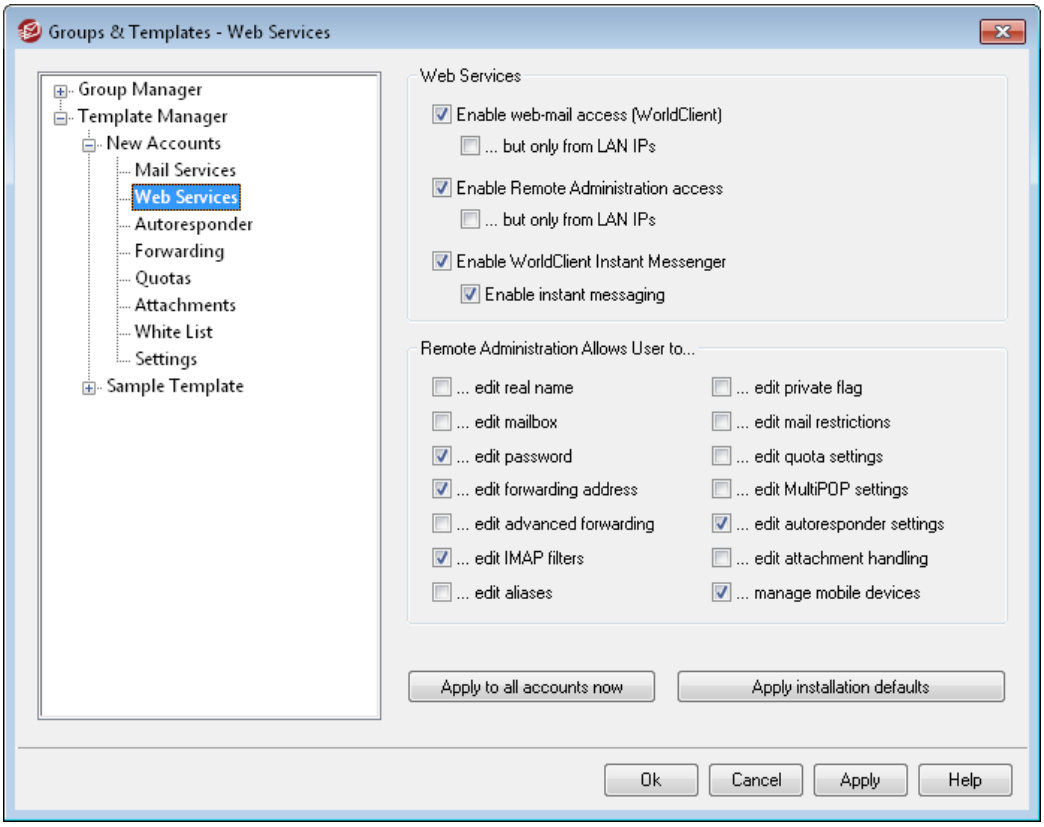
Enable ActiveSync
This option is only available on the New Accounts template. Check this box if you wish to allow new accounts to use ActiveSync on a mobile device to synchronize email, contacts, calendar, and other data with MDaemon/WorldClient.

See:

Template Properties 582
Group Properties 577
New Accounts Template 581
Account Editor » Mail Services 525

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.2.2.1.2 Web Services



The options on this template screen correspond to the options located on the Account Editor's Web Services 526 screen. When a template is set to control this screen 582, it will control the Web Services options for any account belonging to a Group 577 that utilizes the template.

Web Service

Enable web-mail access (WorldClient)
Enable this checkbox if you want accounts controlled by this template to be able to access WorldClient 224, which enables users to access their email, calendars, and other features using a web browser.

...but only from LAN IPs
Check this box if you wish to allow associated accounts access to WorldClient only when connecting from a LAN IP address 514.

Enable Remote Administration access
Check this box if you wish to allow accounts controlled by this template to modify some of their account settings via Remote Administration 251. The accounts will only be able to edit those settings that you designate below.

When this feature is enabled and the Remote Administration server is active, the user will be able to log in to Remote Administration by pointing a browser to the designated MDaemon domain and port assigned to Remote Administration 252 (e.g.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

`http://example.com:1000`). He will first be presented with a sign-in screen and then a screen that contains the settings that he has been given permission to edit. All he needs to do is edit whatever settings he chooses and then click the *Save changes* button. He can then sign out and close the browser. If he has access to WorldClient then he can also access Remote Administration from the Advanced Options menu within WorldClient.

If the user is a Global or Domain Administrator (designated on the Account Editor's Administrative Roles 570 screen) he will see a different screen after he logs in to Remote Administration.

...but only from LAN IPs
Check this box if you wish to allow the account access to Remote Administration only when connecting from a LAN IP address 514.

Enable WorldClient Instant Messenger
Click this box if you wish to enable WCIM 225 support by default for new accounts. This option is only available on the New Accounts Template 581. There is a similar option on Group Properties 577 that can be used to control group member access to WCIM.

Enable Instant Messaging
Click this option is you wish to enable support for WCIM's instant messaging system by default for new accounts. This option is only available on the New Accounts Template 581. There is a similar option on Group Properties 577 that can be used to control group member access to Instant Messaging.

Remote Administration Allows User to...

...edit real name
Enabling this feature will allow accounts associated with this template to modify the *First and last name* 521 setting.

...edit mailbox
Enabling this feature will allow users to modify the *Mailbox name* 521.

Because the *Mailbox name* is part of the account's email address, which is the unique identifier and login value for the account, changing it means that the user will be changing his or her actual email address. This could result in any future messages directed to the old address being rejected, deleted, or the like.

...edit password
Click this checkbox if you wish to allow accounts to modify the *Mailbox password*. For more on password requirements, see: Passwords 636.

...edit forwarding address
When this feature is enabled, accounts associated with the template will be able to modify the forwarding 533 address settings.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...edit advanced forwarding
When this feature is enabled, users will be able to modify the *Advanced Forwarding Settings* 533.

...edit IMAP filters
Use this control to allow each user to create and manage his own IMAP Filters 541. This feature is only available in MDaemon PRO.

...edit aliases
Enable this option if you wish to allow the account holders to use Remote Administration to edit Aliases 546 associated with their accounts.

...edit private flag
This option governs whether or not each will be permitted to use Remote Administration to edit the "*Account is private*" option located on the Account Editor's Settings 573 screen.

...edit mail restrictions
This checkbox controls whether or not the account will be able to edit the Inbound/Outbound mail restriction, located on the Restrictions 534 screen.

...edit quota settings
Click this checkbox if you wish to allow the account to modify the Quota 537 settings.

...edit MultiPOP settings
Click this checkbox if you wish to give the account permission to add new MultiPOP 544 entries and to enable/disable MultiPOP collection for those entries.

...edit autoresponder settings
Click this checkbox if you wish to give the user permission to add, edit, or delete Autoresponders 529 for his account.

...edit attachment handling
Check this box if you wish to allow the user to edit the account's attachment handling options, located on the Attachments 539 screen.

...manage mobile device
Click this option if you wish to allow the account holder to use Remote Administration to manage his or her device-specific settings, such as for BlackBerry and ActiveSync devices.

Apply to all accounts now

This option is only available on the New Accounts Template 581. Click it to apply the settings on this screen to all existing MDaemon accounts that are not specifically controlled by a Web Services Account Template.

Apply installation defaults

This option is only available on the New Accounts Template 581. Click it to reset the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

New Accounts template to the installation defaults. It will only change the template's settings, it will not change any existing accounts.

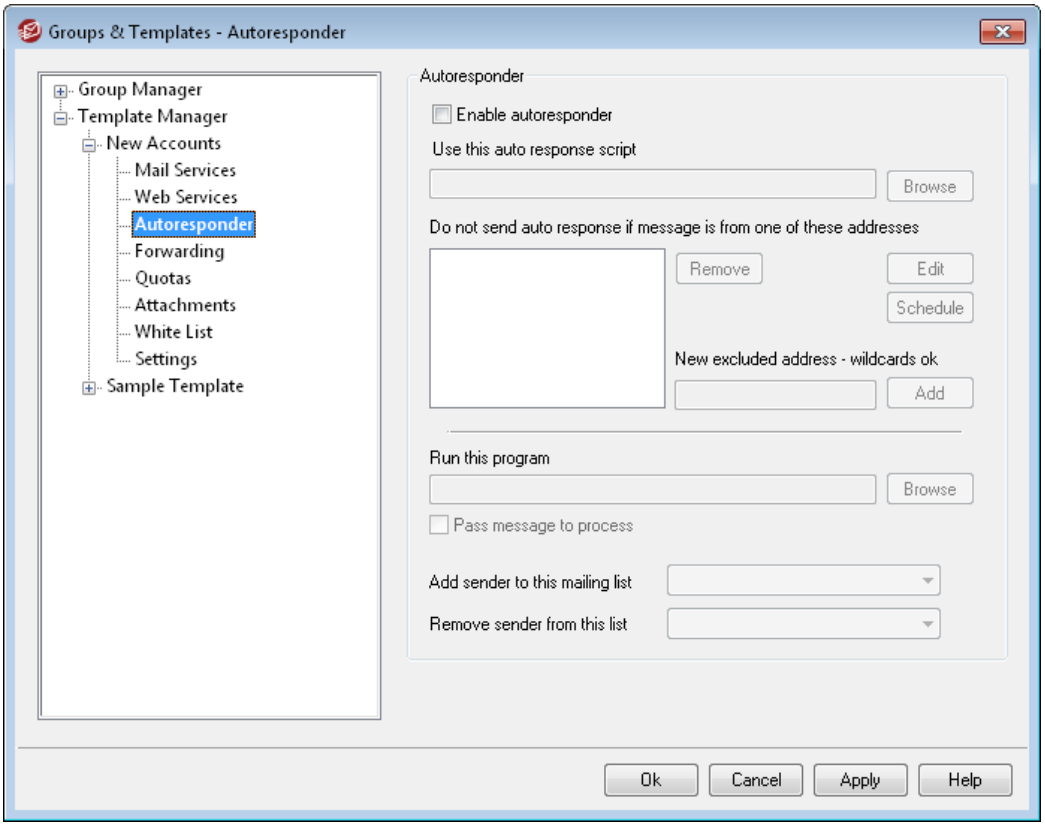
Load "New Accounts" template settings

This option is only available for custom templates. Click it to set the options on this screen to the default values designated on the Web Services screen of the New Accounts Template 581.

See:

Template Properties 582
Group Properties 577
New Accounts Template 581
Account Editor » Web Services 526

5.2.2.1.3 Autoresponder



The options on this template screen correspond to the options located on the Account Editor's Autoresponder 529 screen. When a template is set to control this screen 582, it will control the Autoresponder options for any account belonging to a Group 577 that utilizes the template.

Autoresponders are useful tools for causing incoming email messages to trigger certain

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

events automatically, such as running a program, adding the sender to a mailing list, responding with an automatically generated message, and more. The most common use of autoresponders is to reply to incoming messages automatically with a user-defined message stating that the recipient is on vacation, is unavailable, will reply as soon as possible, or the like. MDaemon users with web access 526 to WorldClient 224 or Remote Administration 251 can use the options provided to compose auto response messages for themselves and schedule the dates they will be in use. Finally, automated response messages are based on response scripts 621 (*.RSP files), which support a large number of macros. These macros can be used to cause much of the script's content to be generated dynamically, making autoresponders quite versatile.

Auto response events are always honored when the triggering message is from a remote source. However, for messages originating locally, autoresponders will only be triggered if you enable the *Autoresponders are triggered by intra-domain mail* option, located on the Autoresponders » Settings 620 screen. You can also use an option on that screen to limit auto response messages to one response per sender per day.

Autoresponder

Enable autoresponder
Enable this control to activate an autoresponder for all groups controlled by this template. For more information on autoresponders see: Autoresponders 617.

Use this auto response script
This field is used to specify the path and filename of the response file (*.RSP) that will be processed and used to compose the message that will be returned to the message sender. Response scripts may contain macros that can be used to make response messages dynamic and automate much of their content. See, Creating Auto Response Scripts 621 for more information.

Do not send auto response if message is from one of these addresses
Here you can list addresses that you wish to be excluded from responses initiated by this autoresponder.

Occasionally auto response messages may be sent to an address that returns an auto response of its own. This can create a "ping-pong" effect causing messages to be continually passed back and forth between the two servers. If you encounter one of those addresses, enter it here to prevent that from happening. There is also an option located on the Autoresponders » Settings 620 screen, which can be used to limit auto response messages to one response per sender per day.

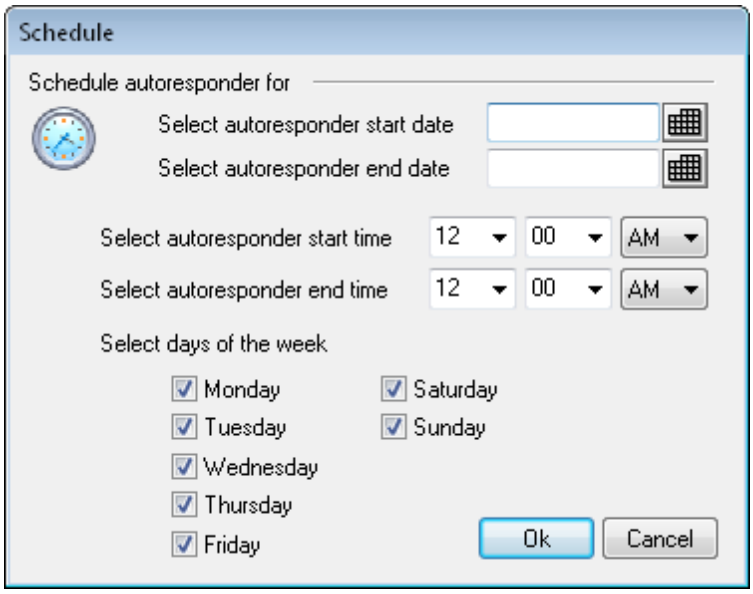
Remove
Click this button to delete any selected entries from the list of excluded addresses.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

New excluded address—wildcards okay
If you wish to add an address to the list of excluded addresses enter it here and then click the *Add* button.

Edit
Click this button to open and edit your selected Auto Response Script.

Schedule
Click this button to open the Schedule dialog on which you can set a start and end date and time for the Autoresponder to be active. Leave the Schedule blank if you want the Autoresponder to be active continually.



Run a Program

Run this program
Use this field to specify the path and filename to a program that you wish to run when new mail arrives for a group member controlled by this template. Care must be taken to ensure that this program terminates properly and can run unattended. Optional command line parameters can be entered immediately following the executable path if desired.

Pass message to process
Select this option and the process specified in the *Run this Program* field will be passed the name of the triggering message as the first available command line parameter. When the autoresponder is set for an account that is forwarding mail to another location and **not** retaining a local copy in its own mailbox (see Forwarding 533) then this function will be disabled.

By default, MDaemon will place the name of the message file as the last parameter on the command line. You can override this behavior by using the `$MESSAGE$` macro. Use this macro in

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

place of where the message file name should be placed. This allows more flexibility in the use of this feature since a complex command line such as this will be possible: `logmail /e /j /message=$MESSAGE$ /q`.

Mailing Lists

Add sender to this mailing list
If a mailing list is entered in this field then the sender of the incoming message will be automatically added as a member of that mailing list. This is a handy feature for building lists automatically.

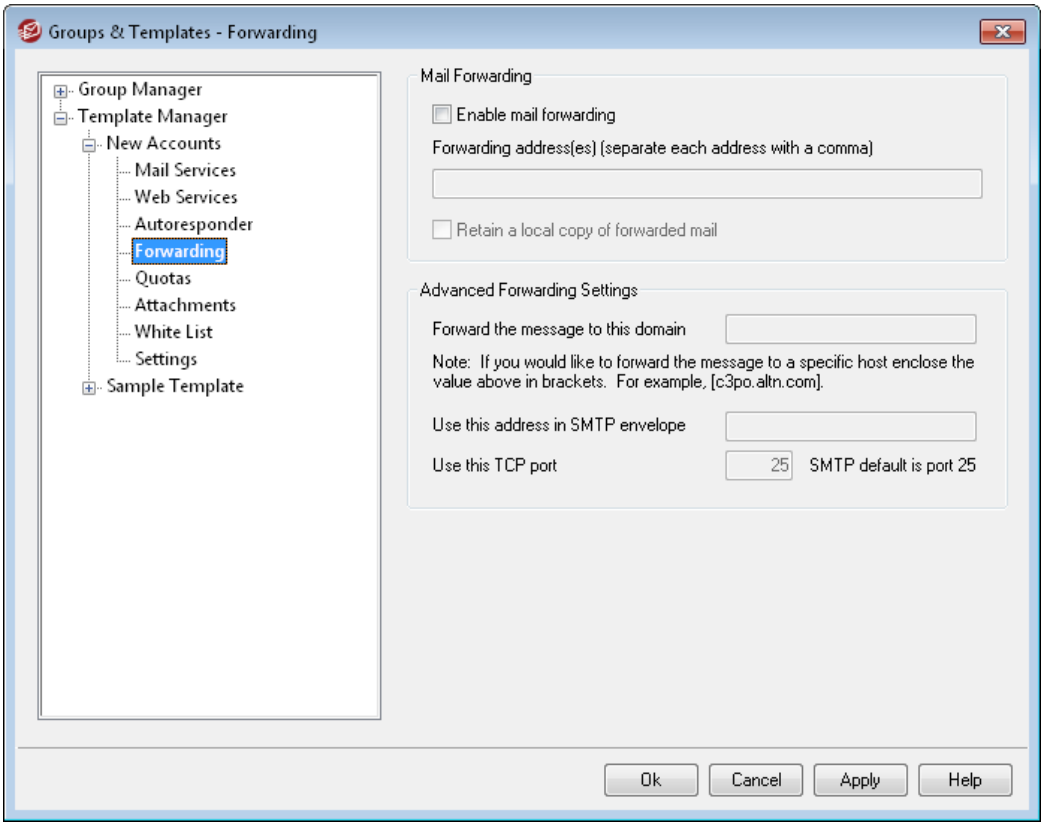
Remove sender from this mailing list
If a mailing list is entered in this field then the sender of the incoming message will be automatically removed from the specified mailing list.

See:

Template Properties 582
Group Properties 577
New Accounts Template 581
Account Editor » Autoresponder 529

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.2.2.1.4 Forwarding



The options on this template screen correspond to the options located on the Account Editor's Forwarding 533 screen. When a template is set to control this screen 582, it will control the Forwarding options for any account belonging to a Group 577 that utilizes the template.

Mail Forwarding

Enable mail forwarding
Check this box if you wish to forward associated accounts' incoming messages to the address or addresses specified in the *Forwarding addresses* option below. MDaemon users with web access 526 to WorldClient 224 or Remote Administration 251 can use the options provided to set the forwarding options for themselves rather than requiring an administrator to do so.

Forwarding addresses (separate each address with a comma)
Use this field to designate any email addresses to which you wish to forward copies of the associated account's incoming messages as they arrive. A copy of each new message arriving at the server will be automatically generated and forwarded to the addresses specified in this field, provided the *Enable mail forwarding* option above is checked. When forwarding to multiple addresses, separate each one with a comma.

Retain a local copy of forwarded mail
By default, a copy of each forwarded message is delivered normally to the local user's mailbox. If you uncheck this box then no local copy will be retained.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Advanced Forwarding Settings

Forward the message to this domain
If you wish to route the forwarded messages through a particular domain's MX servers, then specify that domain here. If you wish to route the messages to a specific host, then enclose the value in brackets (e.g. [host1.example.com]).

Use this address in SMTP envelope
If an address is specified here, it will be used in the "MAIL From" statement sent during the SMTP session with the accepting host, instead of using the actual sender of the message. If you require an empty SMTP "MAIL From" statement (i.e. "MAIL FROM <>") then enter "[trash]" into this option.

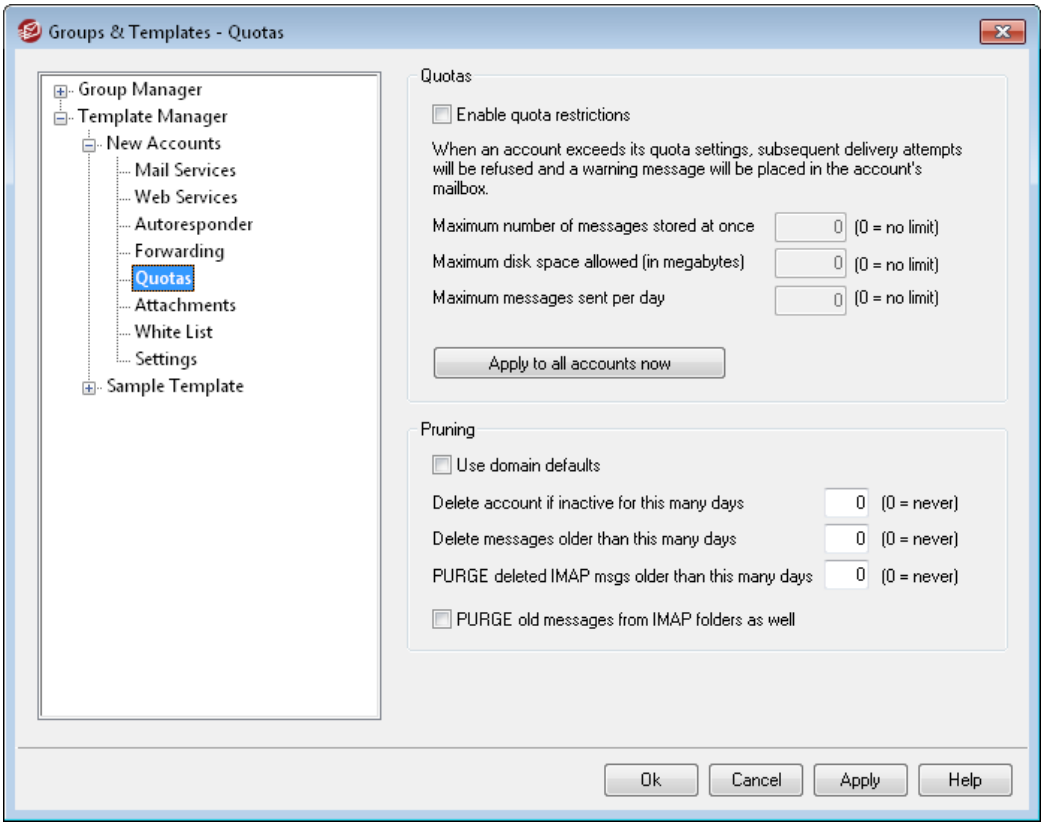
Use this TCP port
MDaemon will send the forwarded messages using the TCP port specified here. The default SMTP port is 25.

See:

Template Properties 582
Group Properties 577
New Accounts Template 581
Account Editor » Forwarding 533

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.2.2.1.5 Quotas



The options on this template screen correspond to the options located on the Account Editor's Quotas 537 screen. When a template is set to control this screen 582, it will control the Quotas options for any account belonging to a Group 577 that utilizes the template.

Quotas

Enable quota restrictions
Check this box if you wish to specify a maximum number of messages that accounts controlled by this template can store, set a maximum amount of disk space that the accounts can use (including any file attachments in each account's Documents folder), or designate a maximum number of messages that the accounts can send via SMTP per day. If a mail delivery is attempted that would exceed the maximum message or disk space limitations, the message will be refused and an appropriate warning message will be placed in the user's mailbox. If a MultiPOP 544 collection would exceed the account's maximum a similar warning is issued and the account's MultiPOP entries are automatically switched off (but not removed from the database).

Use the *Send quota warning emails to accounts nearing the limit* option at "Accounts » Account Settings » Quotas 596" to cause a warning message to be sent when an account nears its quota limits. When the account exceeds a designated

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

> percentage value of either its *Maximum number of messages stored at once* or *Maximum disk space allowed* restriction, a warning message will be sent to the account at midnight. The message will list the account's number of stored messages, the size of its mailbox, and the percent used and remaining. Further, if an existing warning is found in the account's mailbox it will be replaced with an updated message.

Maximum number of messages stored at once
Use this option to designate the maximum number of messages that can be stored for the accounts. Using "0" in the option means there will be no limit to the number of messages permitted.

Maximum disk space allowed (in megabytes)
Use this option to designate the maximum amount of disk space that the accounts can use, including any file attachments that may be stored in each account's Documents folder. Using "0" in the option means there will be no limit to the amount of disk space that the accounts can use.

Maximum messages sent per day
Use this option to designate the maximum number of messages that each account can send per day via SMTP. If the account reaches this limit then new mail from the account will be refused until the counter is reset at midnight. Use "0" in the option if you do not wish to limit the number of messages the account can send.

Apply to all accounts now

Click this button to apply the settings on this screen to all existing MDaemon accounts whose Quotas settings are not specifically controlled by an account template. This will reset the accounts to the default Quotas values. This option is only available on the New Accounts Template 581.

Pruning

The options in this section are used to designate when or if an account controlled by this template will be deleted if it becomes inactive. You can also designate whether or not old messages belonging to the account will be deleted after a certain amount of time. Each day at midnight, MDaemon will remove all messages that have exceeded the time limits stated, or it will delete the account completely if it has reached the inactivity limit.

Use domain defaults
The default Pruning settings are domain-specific and located on the Domain Manager's Settings 140 screen. If you wish to override the domain defaults for template-controlled accounts, clear this checkbox and set the desired values in the options below.

Delete account if inactive for this many days (0 = never)
Specify the number of days that you wish to allow the account to be inactive before it will be deleted. A value of "0" in this control means that the account

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

will never be deleted due to inactivity.

Delete messages older than this many days (0 = never)
This is the number of days that any given message may reside in the account's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age.

PURGE deleted IMAP msgs older than this many days (0 = never)
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in a user's folders. Messages flagged for deletion longer than this number of days will be purged. A value of "0" means that messages flagged for deletion will never be purged due to their age.

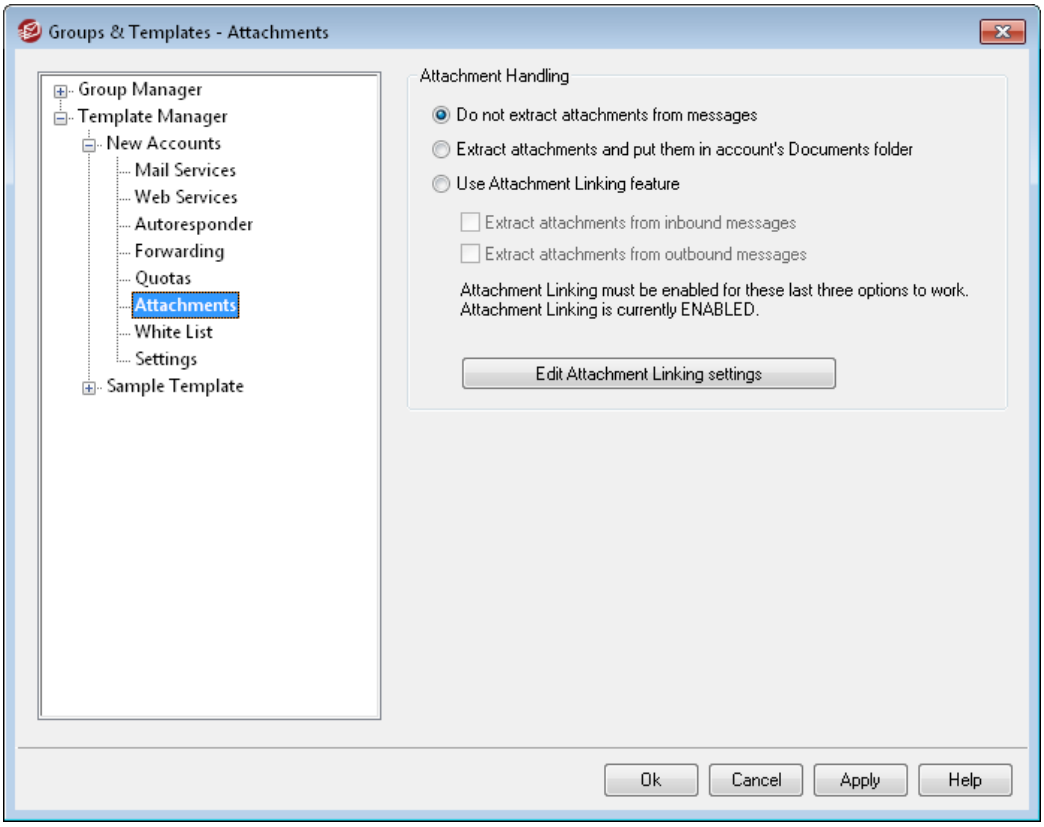
PURGE old messages from IMAP folders as well
Click this checkbox if you want the "*Delete messages older than...*" option to apply to messages in IMAP folders as well. When this option is disabled, messages contained in IMAP folders will not be deleted, regardless of their age.

See:

Template Properties 582
Group Properties 577
New Accounts Template 581
Account Editor » Quotas 537
Account Settings » Quotas 638

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.2.2.1.6 Attachments



The options on this template screen correspond to the options located on the Account Editor's Attachments 539 screen. When a template is set to control this screen 582, it will control the Attachments options for any account belonging to a Group 577 that utilizes the template.

Attachment Handling

Do not extract attachments from messages
If this option is selected, attachments will not be extracted from a template-controlled account's messages. Messages with attachments will be handled normally, leaving the attachments intact.

Extract attachments and put them in account's Documents folder
If set, this option causes MDaemon to automatically extract any Base64 MIME embedded file attachments found within incoming mail messages for the account. Extracted files are removed from the incoming message, decoded, and placed in the account's Documents folder. A note is then placed within the body of the message, stating the names of the files that were extracted. This option does not provide a link to the stored attachments, but users can use WorldClient 224 to access their Documents folder.

Use Attachment Linking feature
Select this option if you wish to use the Attachment Linking feature for inbound or outbound messages with attachments.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

If this option is selected but the Attachment Linking feature is disabled on the Attachment Linking 262 dialog, then attachments will not be extracted.

Extract attachments from inbound messages
When this option is enabled, attachments will be extracted from the account's incoming messages and stored in the location designated on the Attachment Linking 262 dialog. URL links are then placed within the body of the message, which the user can then click to download the files. For security these URL links do not contain direct file paths. Instead they contain a unique identifier (GUID) that the server uses to map the file to the actual path. This GUID map is stored in the `AttachmentLinking.dat` file..

Extract attachments from outbound messages
Check this box if you wish to use the Attachment Linking feature to extract attachments from the account's outbound messages. When the account sends an email, Attachment Linking will extract the file, store it, and replace it with a URL to download the file.

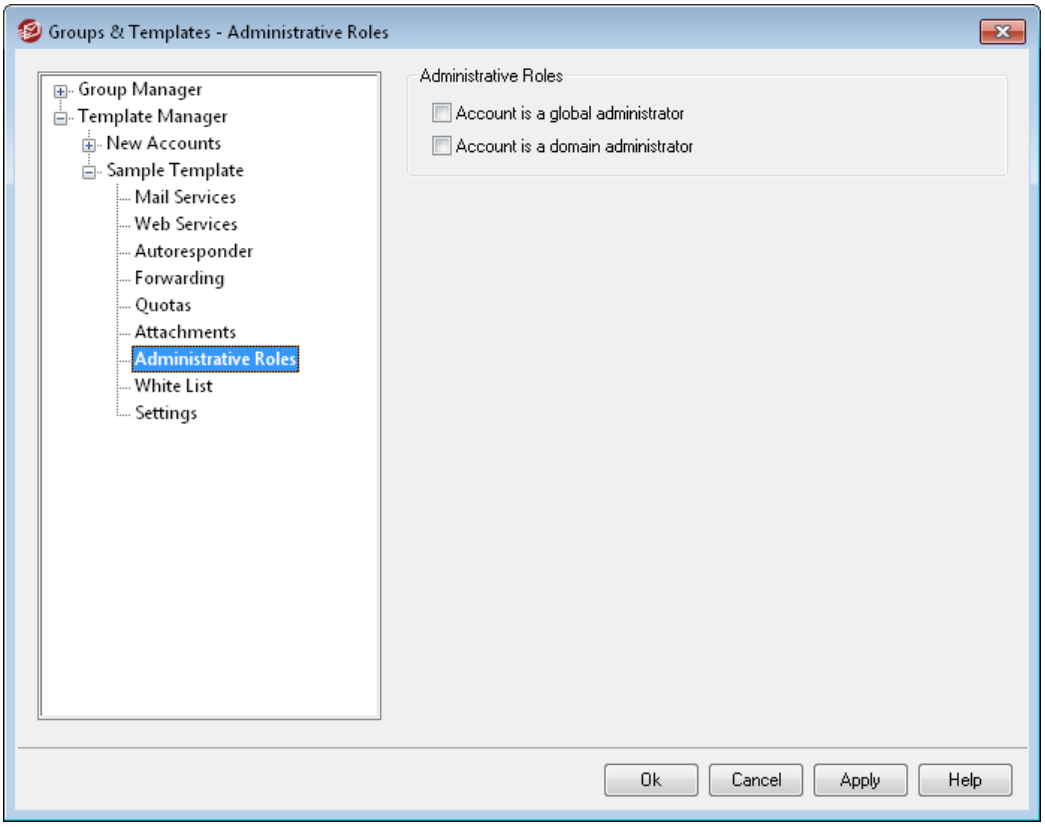
Edit Attachment Linking settings
Click this button to open the Attachment Linking 262 dialog.

See:

Template Properties 582
Group Properties 577
New Accounts Template 581
Attachment Linking 524
Account Editor » Attachments 539

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.2.2.1.7 Administrative Roles



Administrative Roles

Account is a global administrator
Enable this checkbox to grant these users server-level administrative access. Global administrators have:

- Full access to server configuration, all users, and all domains via Remote Administration
- Access to all MDaemon users of all MDaemon domains as Instant Messaging buddies.
- The ability to post to all mailing lists even if flagged as "Read Only".
- The ability to post to all mailing lists even if not a member.

The user will have complete access to MDaemon's files and options. For more on the administrative options within the Remote Administration web-interface, see Remote Administration 251.

Account is a domain administrator
Click this checkbox to designate the users as Domain Administrators. Domain administrators are similar to global administrators except that their administrative access is limited to this domain and to the permissions granted on the Web Services 526 page.

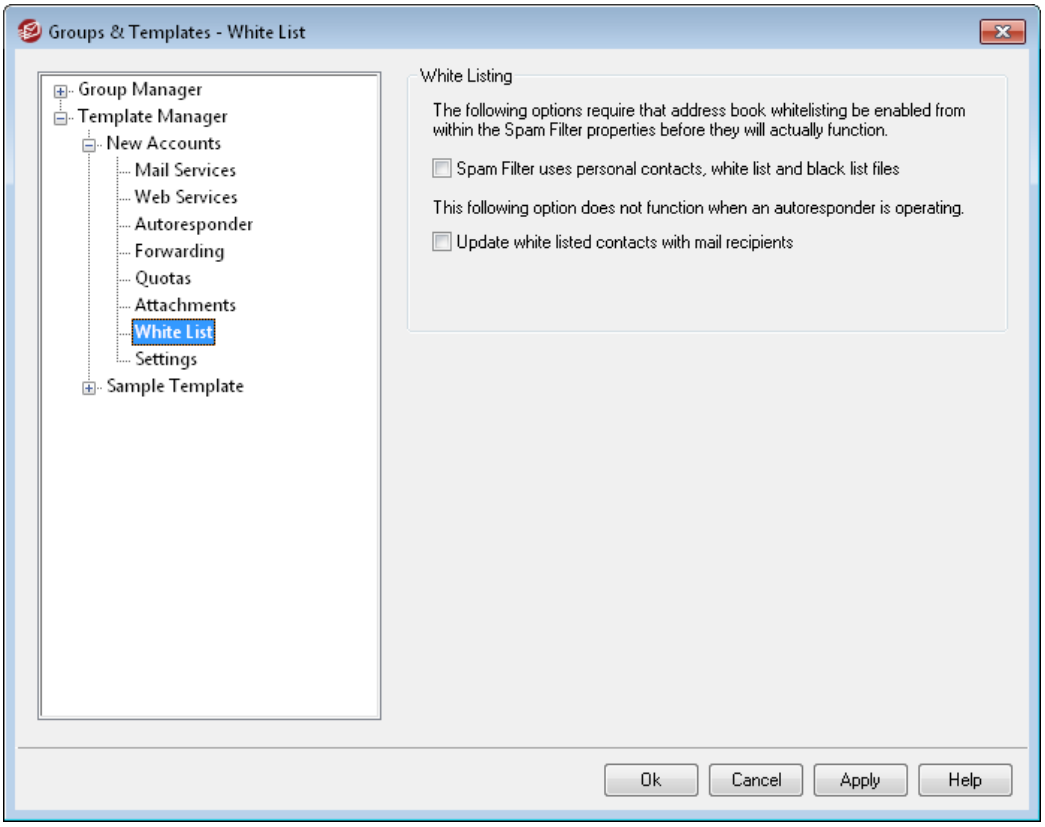
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

This screen is not available on the New Accounts template[581]. Administrative access cannot be automatically granted to new accounts. To grant administrative access to an account, associate the account with a customized template that uses this screen to grant that access, or manually designate the account as an administrator from the Account Editor's Administrative Roles[570] screen.

See:

Template Properties[582]
Group Properties[577]
New Accounts Template[581]
Account Editor » Administrative Roles[570]

5.2.2.1.8 White List



The options on this template screen correspond to the settings located on the Account Editor's White List[571] screen. When a template is set to control this screen[582], it will control the White List screen settings for any account belonging to a Group[577] that utilizes the template.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

White Listing

Spam Filter uses personal contacts, white list, and black list files
The Spam Filter's White List (automatic) 413 screen contains a global option that can be used to cause the Spam Filter to white list a message automatically when the sender of the message is found in the local recipient's personal contacts or white list folder. It will also automatically black list a message when the sender is found in the user's black list file. If you have enabled the Spam Filter's global option but do not wish to apply it to these accounts, clear this check box to override the global setting. If the global option is disabled then this option will not be available.

Keeping your contacts updated and synchronized with WorldClient, the Windows Address Book, and other MAPI mail clients that use the Windows Address Book can be easily done using WorldClient Instant Messenger 227.

Update white listed contacts with mail recipients
Click this option if you wish to update each account's white list folder each time it sends an outgoing message to a non-local email addresses. When used in conjunction with the above option, *Spam Filter uses personal contacts, white list, and black list files*, the number of Spam Filter false positives can be drastically reduced. The *Automatically update white listed contacts* option located on the White List (automatic) 413 screen must be enabled before you can use this feature.

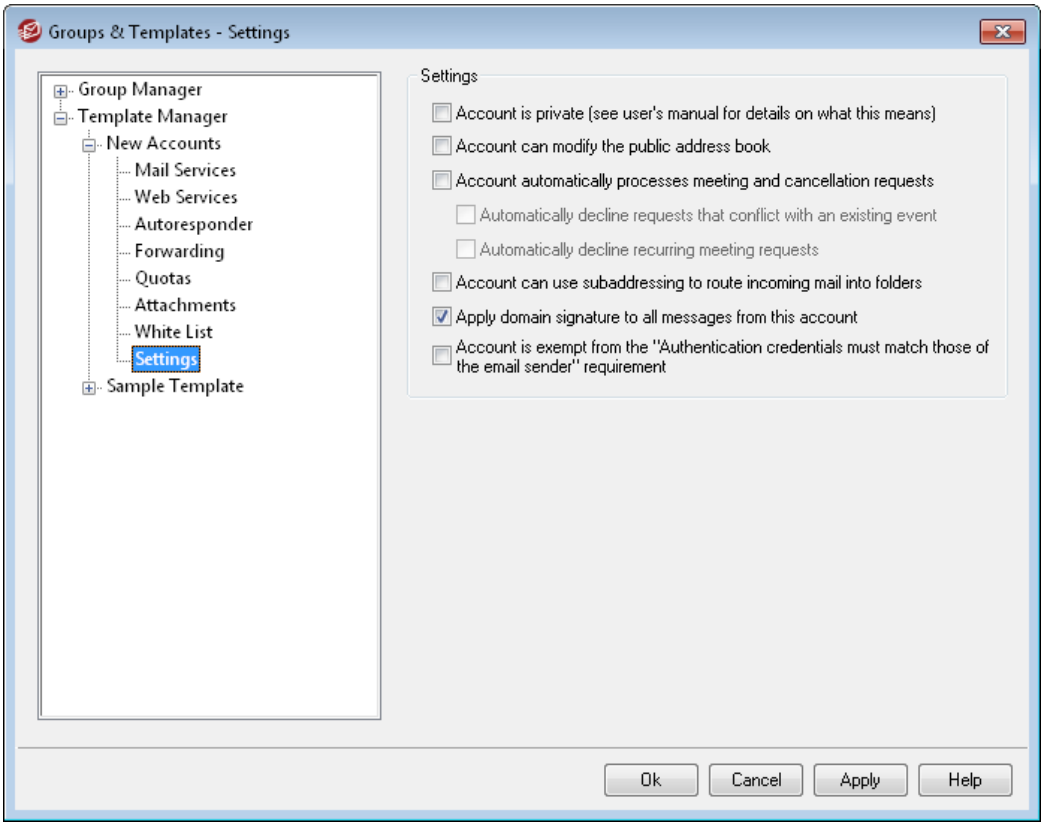
This option is disabled when the account is using an autoresponder.

See:

Template Properties 582
Group Properties 577
New Accounts Template 581
Account Editor » White List 571

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.2.2.1.9 Settings


Groups & Templates - Settings
Group Manager
Template Manager
New Accounts
Mail Services
Web Services
Autoresponder
Forwarding
Quotas
Attachments
White List
Settings
Sample Template
Settings
Account is private (see user's manual for details on what this means)
Account can modify the public address book
Account automatically processes meeting and cancellation requests
Automatically decline requests that conflict with an existing event
Automatically decline recurring meeting requests
Account can use subaddressing to route incoming mail into folders
Apply domain signature to all messages from this account
Account is exempt from the "Authentication credentials must match those of the email sender" requirement
Ok
Cancel
Apply
Help

The options on this template screen correspond to the settings located on the Account Editor's Settings 573 screen. When a template is set to control this screen 582, it will control the Settings screen for any account belonging to a Group 577 that utilizes the template.

Settings

Account is private
MDaemon automatically creates and maintains an "everyone@" mailing list for each domain, which can be used to send a message to everyone at once. By default MDaemon will include all accounts when it constructs this list. Check this box if you wish to exclude accounts controlled by this template from that list. This will also hide the accounts from shared calendars and VRFY 53 results. Each account's address book entry, however, will not be hidden from a global address book lookup performed on a BlackBerry device that is activated on your MDaemon's BlackBerry Enterprise Server.

Account can modify the public address book
Click this option if you want the accounts to be able to add and delete entries from the WorldClient or LDAP-based public address books.

If an Account is synchronizing folders with WorldClient Instant Messenger 227 then modifications could be propagated to all

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

users. Exercise caution when enabling this feature.

Account automatically processes meeting and cancellation requests
Click this checkbox if you wish to cause automatic processing of meeting requests, changes, and cancellations for each account. When an account receives a message that contains a meeting request, the account's calendar will be updated automatically. This option is disabled for all accounts by default.

Automatically decline requests that conflict with an existing event
If automatic processing of meeting requests and cancellations is enabled, those meeting requests will be automatically declined by default when they conflict with an existing event. Clear this checkbox if you wish to allow the conflicting event to be created.

Automatically decline recurring meeting requests
Click this box if automatic processing of meeting requests and cancellations is enabled but you wish to decline those requests when they are for recurring meetings.

Account can use subaddressing to route incoming mail into folders
Click this checkbox if you wish to permit subaddressing 574 for the accounts.

Apply domain signature to all messages from this account
When there is a Domain Signature 138 for the domain to which accounts governed by this template belong, this option causes it to be added to all emails sent by those accounts.

Account is exempt from the "Authentication credentials must match those of the email sender" requirement
Use this option if you wish to exempt accounts governed by this template from the "*Authentication credentials must match those of the email sender*" global option located on the SMTP Authentication 442 screen.

See:

Template Properties 582
Group Properties 577
New Accounts Template 581
Account Editor » Settings 573

5.3 Account Settings

5.3.1 Active Directory

Using the Active Directory options located at Accounts » Account Settings » Active Directory, MDaemon can be configured to monitor Active Directory and automatically

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

create, edit, delete and disable MDaemon accounts when their associated accounts are altered in Active Directory. Further, it can also be set to keep all public contact records updated with the most recent information stored in Active Directory. Common fields like an account's postal address, phone numbers, business contact information, and so on can be populated into the public contact records and updated any time they are changed in Active Directory.

Creating Accounts

When set to monitor Active Directory, MDaemon will query for changes at a designated interval and then create a new MDaemon user account whenever it finds that a new Active Directory account has been added. This new MDaemon user account will be created using the full name, logon, mailbox, description, and enabled/disabled state found within Active Directory.

By default, new MDaemon accounts created as a result of Active Directory monitoring will be added to MDaemon's Default Domain. Alternatively, you can choose to have those accounts added to the domain found within the account's "`UserPrincipalName`" Active Directory attribute. When using this option, if an account requires a domain that doesn't yet exist within MDaemon, a new domain 121 will be created automatically.

Deleting Accounts

MDaemon can be configured to take one of the following actions when an account is deleted from Active Directory: do nothing, delete the associated MDaemon account, disable the associated MDaemon account, or freeze the associated MDaemon account (i.e. the account can still receive mail but the user can't collect it or access it).

Updating Accounts

When MDaemon detects changes to Active Directory accounts, it will automatically update the associated properties in the matching MDaemon account.

Synchronizing MDaemon with Active Directory

A "*Perform full AD scan now*" option is available to cause MDaemon to query the Active Directory database and then create or modify MDaemon user accounts as necessary. When an Active Directory account is found that matches an already existing MDaemon account, the MDaemon account will be linked to it. Then, any future changes made to the Active Directory accounts will be propagated to the MDaemon accounts automatically.

Dynamic Authentication

Accounts created by MDaemon's Active Directory feature will be setup for Dynamic Authentication by default. With Dynamic Authentication, MDaemon has no need to store the account's password within its own user database. Instead, the account holder will use his or her Windows login/password credentials and MDaemon will pass those to Windows for authentication of the associated account.

To use Dynamic Authentication with Active Directory, a Windows domain name must be present in the space provided on the Monitoring 608. This is the Windows domain that MDaemon will use when attempting to authenticate accounts. In most cases, MDaemon will detect this Windows domain name automatically and fill it in for you. However, you

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

can use an alternate domain in this option if you choose, or you can use "NT_ANY" if you wish to allow authentication across all of your Windows domains instead of limiting it to a specific one. If you leave this option blank then MDaemon will not use Dynamic Authentication when new accounts are created. Instead it will generate a random password, which you will have to edit manually before users will be able to access their mail accounts.

Persistent Monitoring

Active Directory monitoring will continue to work even when MDaemon is shut down. All Active Directory changes will be tracked and then MDaemon will process them once it restarts.

Active Directory File Security

It is worth noting that MDaemon's Active Directory features do not alter the Active Directory schema files in any way — all monitoring is one-way from Active Directory to MDaemon. MDaemon will not alter your directory.

Active Directory Template

Whenever MDaemon adds or makes changes to accounts due to Active Directory monitoring and scanning, it will use an Active Directory template ("/app/ActiveDS.dat") to link certain Active Directory attribute names to MDaemon's account fields. For example, MDaemon links the Active Directory attribute "cn" to MDaemon's "FullName" field by default. These links, however, are not hard-coded. You can easily edit this template with Notepad if desired and alter any of the default field mappings. For example, "FullName=%givenName% %sn%" could be used as a replacement for the default setting: "FullName=%cn%". See ActiveDS.dat for more information.

Updating the Public Address Books

Active Directory monitoring can be used to periodically query Active Directory and keep all public contact records in MDaemon updated with the most recent information. Common fields like an account's postal address, phone numbers, business contact information, and so on will be populated into their public contact record, and this data will be updated any time it is changed in Active Directory. To enable this feature, use the "*Monitor Active Directory and update public address book(s)*" option located at: Active Directory » Monitoring 608.

Numerous contact record fields can be monitored using this feature. For a complete list of which public contact record fields can be mapped to Active Directory attributes, see the ActiveDS.dat file. This file has several new mapping templates which allow you to specify one or more Active Directory attributes from which to populate a particular contact record field (for example, %fullName% for the fullname field, %streetAddress% for the street address field, and so on).

MDaemon must match an account's email address to some attribute within Active Directory in order to know which contact record to update. If it can't find such a match it does nothing. By default MDaemon will try to construct an email address using the data taken from the attribute mapped to the Mailbox template (see ActiveDS.dat) to which MDaemon will internally append the default domain 121 name, just as it would when actually creating and deleting accounts based on Active Directory data.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

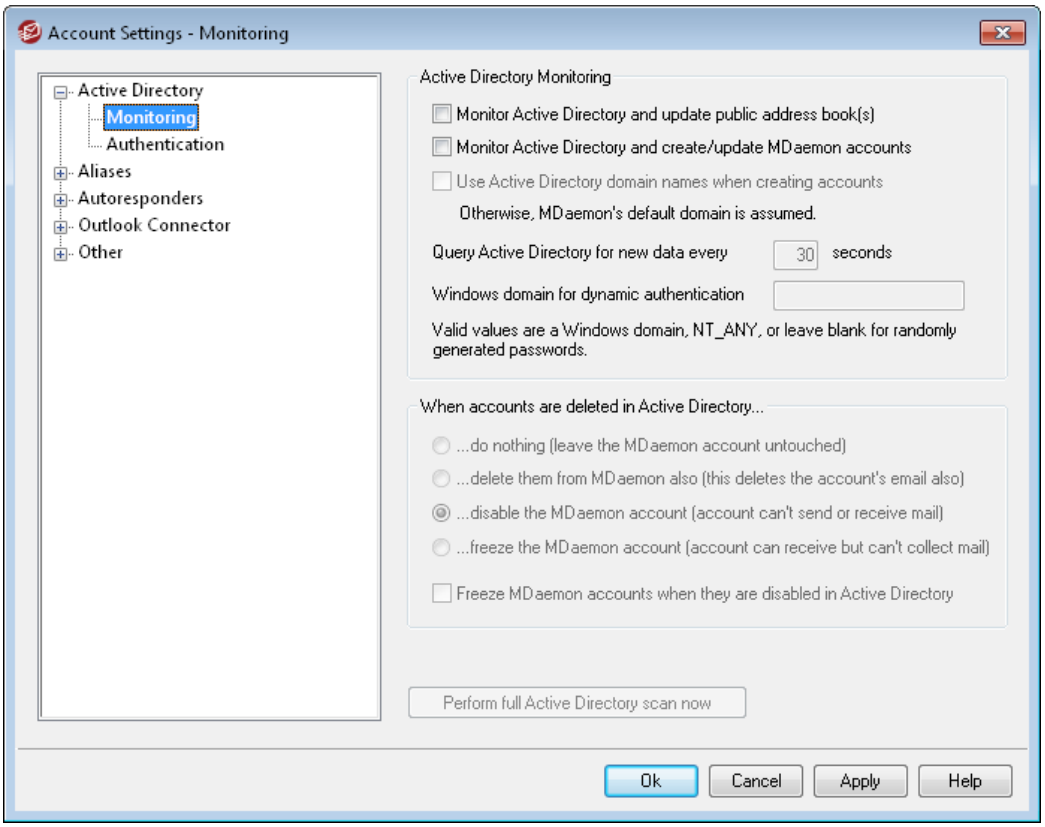
However, you can uncomment the "abMappingEmail" template inside `ActiveDS.dat` and tie it to any Active Directory attribute you wish (like `%mail%`, for example). However, please note that the value of this attribute must contain an email address that will be recognized as a valid local user account.

This feature will create the contact records on the fly if they don't already exist and it will update contact records that do exist. Further, please note that it will overwrite any changes you make outside of Active Directory. Contact record fields that are not mapped are left unaltered. Therefore any existing data that is not subject to this process will not be altered or lost. Finally, MDaemon accounts that are set to private 573 are not subject to having their contact records created or updated.

See:

Active Directory » Monitoring 608
Active Directory » Authentication 611

5.3.1.1 Monitoring


Account Settings - Monitoring
Active Directory
Monitoring
Authentication
Aliases
Autoresponders
Outlook Connector
Other
Active Directory Monitoring
Monitor Active Directory and update public address book(s)
Monitor Active Directory and create/update MDaemon accounts
Use Active Directory domain names when creating accounts
Otherwise, MDaemon's default domain is assumed.
Query Active Directory for new data every
30
seconds
Windows domain for dynamic authentication
Valid values are a Windows domain, NT_ANY, or leave blank for randomly generated passwords.
When accounts are deleted in Active Directory...
...do nothing (leave the MDaemon account untouched)
...delete them from MDaemon also (this deletes the account's email also)
...disable the MDaemon account (account can't send or receive mail)
...freeze the MDaemon account (account can receive but can't collect mail)
Freeze MDaemon accounts when they are disabled in Active Directory
Perform full Active Directory scan now
Ok
Cancel
Apply
Help

Active Directory Monitoring

Monitor Active Directory and update public address book(s)
Enable this option if you wish to use Active Directory to keep all public contact records updated with the most recent information stored in Active Directory.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Common fields like an account's postal address, phone numbers, business contact information, and so on will be populated into their public contact record and this data will be updated any time it is changed in Active Directory. Numerous contact record fields will be monitored in this way. For a complete list of which public contact record fields can be mapped to Active Directory attributes, see the `ActiveDS.dat` file. See: Updating the Public Address Books 607, for more information.

Monitor Active Directory for user account changes and create/update MDaemon accounts
Click this option to activate Active Directory monitoring, which will create and update MDaemon accounts as Active Directory is updated.

Use Active Directory domain names when creating accounts
Use this option if you would like new accounts created as a result of Active Directory monitoring to be added to the domain found within the account's "`UserPrincipalName`" Active Directory attribute. When using this option, if an account requires a domain that doesn't yet exist within MDaemon, a new domain 121 will be created automatically. Clear/disable this option if you would like all new accounts to be added to MDaemon's Default Domain 121.

Query Active Directory for new data every [XX] seconds
This is the interval at which MDaemon will monitor Active Directory for changes.

Windows domain for dynamic authentication
Specify a Windows domain name here if you wish to use Dynamic Authentication for accounts created by Active Directory monitoring. If you leave this field blank then new accounts will be assigned random passwords. You will then have to edit those passwords manually in order for the accounts to be accessed.

When accounts are deleted in Active Directory...
The option selected below determines the action MDaemon will take when an MDaemon account's associated Active Directory account is deleted.

...do nothing
Choose this option if you do not wish MDaemon to make any changes to an MDaemon account when its associated account is deleted from Active Directory.

...delete them from MDaemon also
Choosing this option will cause the MDaemon account to be deleted when its associated account is deleted from Active Directory.

This will cause the associated MDaemon account to be completely removed. All of the account's messages, message folders, address books, calendars, and so on will be deleted.

...disable the MDaemon account
When this option is selected and an Active Directory account is deleted, its corresponding MDaemon account will be disabled. This means that the MDaemon account will still exist on the server, but it cannot send or receive email or be accessed by anyone.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...freeze the MDaemon account
When this option is selected MDaemon will still accept the account's incoming mail but effectively "lock" it so that it cannot be accessed. In other words, incoming mail addressed to that account will not be rejected or deleted by MDaemon but the account holder will not be able to collect or access that mail as long is the account is frozen.

Freeze MDaemon accounts when they are disabled in Active Directory
By default, when you disable an account in Active Directory, MDaemon will also disable the associated account in MDaemon. This makes the account inaccessible and MDaemon will neither accept nor deliver messages for it. However, if you prefer to have the associated MDaemon account frozen instead of disabled, enable this option. MDaemon will still accept messages for frozen accounts, but users will not be able to access those accounts to collect or send their email.

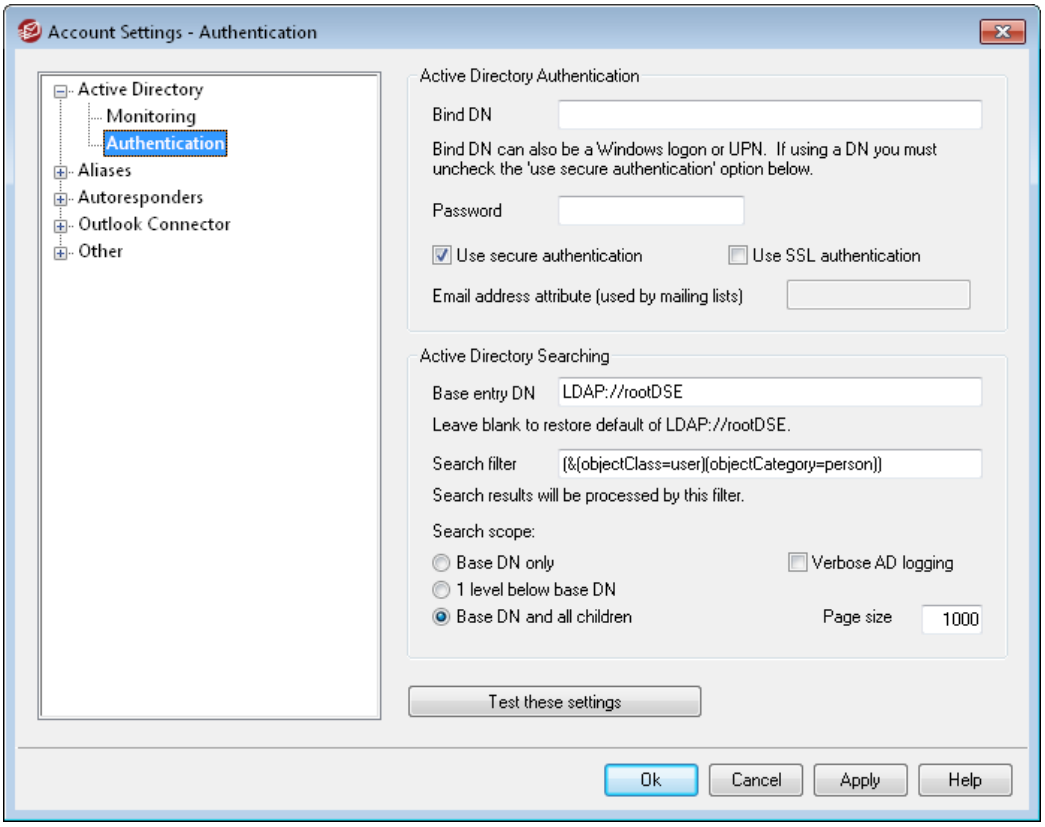
Perform full Active Directory scan now
Click this button to cause MDaemon to query the Active Directory database and then create, edit, or delete accounts as necessary. When an Active Directory account is found that matches an already existing MDaemon account, the MDaemon account will be linked to it.

See:

Active Directory 605
Active Directory » Authentication 611

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.3.1.2 Authentication



Access to Active Directory may require special permissions to be set for all features to function.

Active Directory Authentication

Bind DN
This is the DN that MDaemon will use when binding to Active Directory using LDAP. Active Directory permits the use of a Windows account or UPN when binding.

When using a DN in this option rather than a Windows logon, you must disable/clear the "*Use secure authentication*" option below.

Password
This is the password that corresponds to the DN or Windows logon used in the *Bind DN* option above.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Use secure authentication
Click this checkbox if you wish to use secure authentication when performing your Active Directory searches. You cannot use this option when you are using a DN rather than a Windows logon in the *Bind DN* option above.

Use SSL authentication
Click this checkbox if you wish to use SSL authentication when performing your Active Directory searches.

Use of this option requires an SSL server and infrastructure on your Windows network and Active Directory. Contact your IT department if you are unsure if your network is setup this way, and to find out if you should enable this option.

Email address attribute
This attribute is used for MDaemon mailing lists and is only available when accessing the Active Directory options located on the Mailing Lists 209 dialog.

Active Directory Searching

Base entry DN
This is the Distinguished Name (DN) or starting point in the Directory Information Tree (DIT) at which MDaemon will search your Active Directory for accounts and changes. By default MDaemon will begin searching at Root DSE, which is the topmost entry in your Active Directory hierarchy. Designating a more precise starting point closer to the location of your user accounts in your particular Active Directory tree can reduce the amount of time required to search the DIT for accounts and account changes. Leaving this field blank will restore the default setting of `LDAP://rootDSE`

Search filter
This is the LDAP search filter that will be used when monitoring or searching your Active Directory for accounts and account changes. Use this filter to more precisely locate the desired user accounts that you wish to include in Active Directory monitoring.

Search scope:

This is the scope or extent of your Active Directory searches.

Base DN only
Choose this option if you wish to limit your search to only the base DN specified above. The search will not proceed below that point in your tree (DIT).

1 level below base DN
Use this option if you wish to extend your Active Directory search to one level below the supplied DN in your DIT.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Base DN and all children
This option will extend the scope of your search from the supplied DN to all of its children, down to the lowest child entry in your DIT. This is the default option selected, which when combined with the default Root DSE setting above means that the entire DIT below the Root DSE will be searched.

Page size
If the results of an Active Directory query exceed a specified number of entries, then they will be returned in separate "pages" in order to retrieve all the results. This setting is the maximum number of entries that will be included per page.

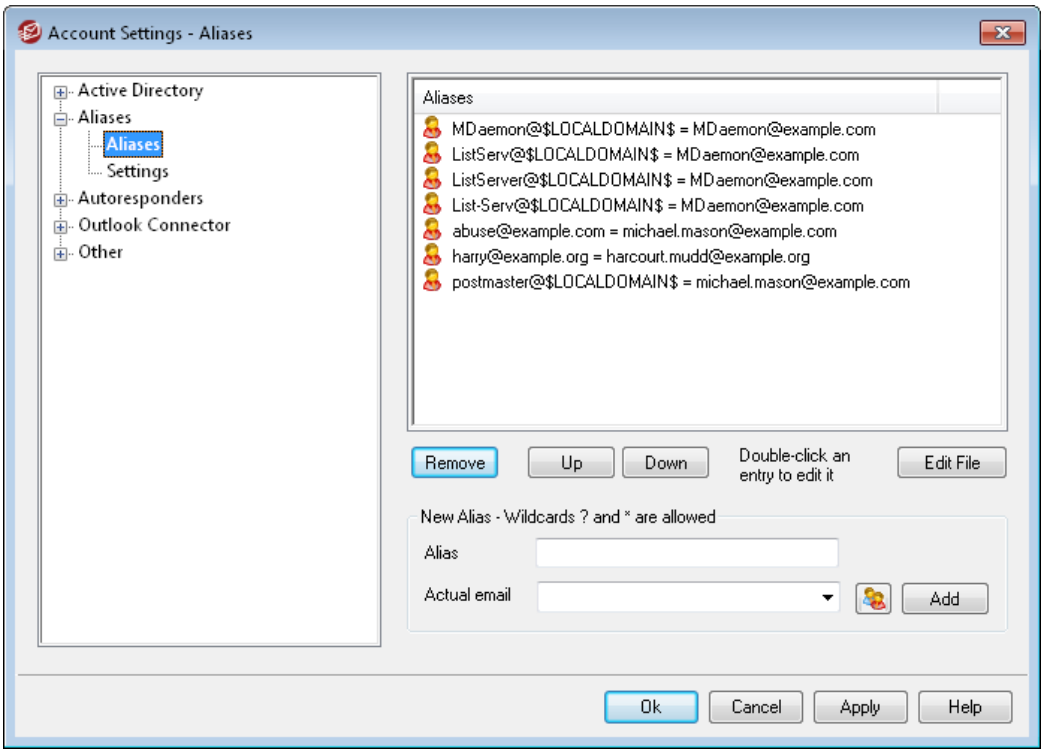
Verbose AD logging
By default MDaemon will use verbose logging for Active Directory. Clear this checkbox if you wish to use less extensive Active Directory logging.

Test these settings

Click this button to test MDaemon's Active Directory configuration.

5.3.2 Aliases

5.3.2.1 Aliases



The Aliases features makes it possible for you to create alternate mailbox names for your accounts or mailing lists, which are useful when you want multiple mailbox names to resolve to a single user account or list. Without aliases you'd have to create separate user accounts for each address and then forward messages or use complicated filter rules to associate them with other accounts.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

For example, if user1@example.com handled all billing inquiries to your domain, but you wanted to tell everyone to send them to billing@example.com, then you could create an Alias so that messages addressed to billing@example.com would actually go to user1@example.com. Or, if you were hosting multiple domains and wanted all messages addressed to the Postmaster (regardless of the domain) to go to user1@example.com, then you could use a wildcard to associate the alias, Postmaster@*, with his address.

Current Aliases

This window contains all current aliases that you have created.

Remove
Click this button to remove a selected entry from the *Current Aliases* list.

Up
Aliases are processed in the order in which they are listed. You can move an alias to a higher position in the list by selecting it and then clicking this button.

Down
Aliases are processed in the order in which they are listed. You can move an alias to a lower position in the list by selecting it and then clicking this button.

Edit File
Click this button if you wish to open the Alias.dat file in a text editor, to manually search or edit it. After making any desired changes, exit the text editor and then MDaemon will reload the file.

Alias
Enter the email address that you wish to be an alias of the "*Actual email*" listed below. Wildcards of "?" and "*" are acceptable, and you can use "@$LOCALDOMAIN$" in the alias as a wildcard that will match only your local domains. For example: "user1@example.*", "*@$LOCALDOMAIN$", and "user1@$LOCALDOMAIN$" are all valid for use in an alias.

Actual email
Select an account from the drop-down list, use the Account icon to browse for an account, or type a new email address or mailing list into this space. This is the actual email address that will receive the message when it is addressed to a corresponding alias.

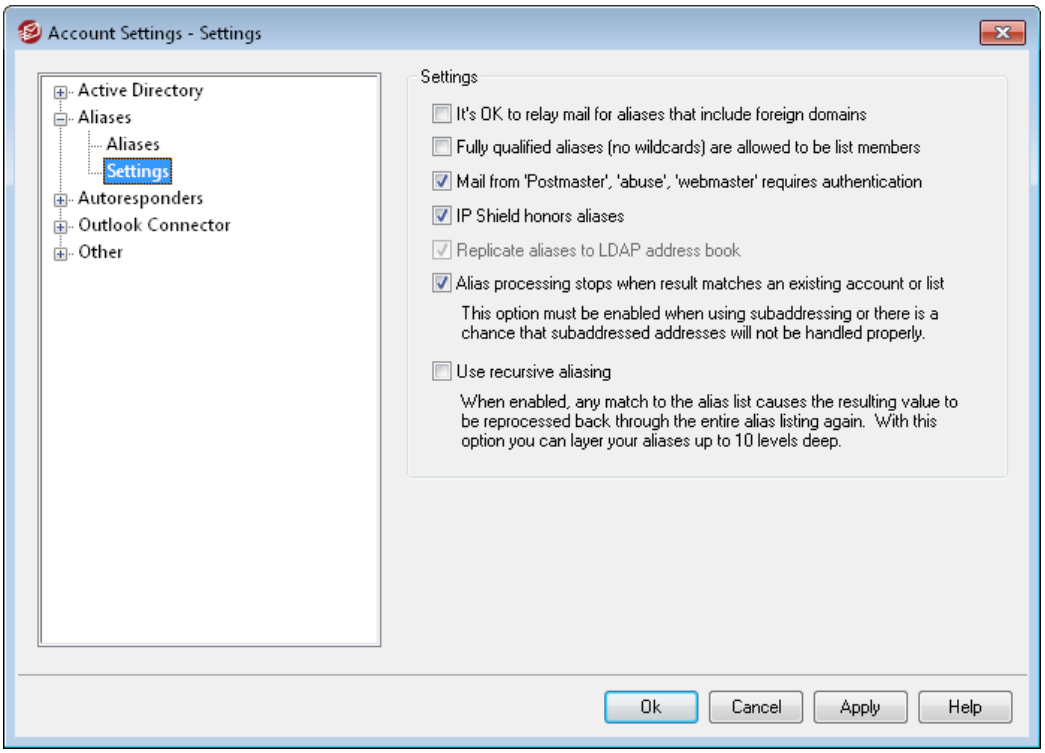
Add
Click the *Add* button to add the alias to the list. The *Alias* and *Actual email* values will be combined and placed in the *Current Aliases* window.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Aliases » Settings 615
Account Editor » Aliases 546

5.3.2.2 Settings


Account Settings - Settings
Active Directory
Aliases
Aliases
Settings
Autoresponders
Outlook Connector
Other
Settings
It's OK to relay mail for aliases that include foreign domains
Fully qualified aliases (no wildcards) are allowed to be list members
Mail from 'Postmaster', 'abuse', 'webmaster' requires authentication
IP Shield honors aliases
Replicate aliases to LDAP address book
Alias processing stops when result matches an existing account or list
This option must be enabled when using subaddressing or there is a chance that subaddressed addresses will not be handled properly.
Use recursive aliasing
When enabled, any match to the alias list causes the resulting value to be reprocessed back through the entire alias listing again. With this option you can layer your aliases up to 10 levels deep.
Ok
Cancel
Apply
Help

Settings

It's OK to relay mail for aliases that include foreign domains
Check this box if you wish to allow MDaemon to relay mail for aliases that include non-local domains. This option overrides the *Do not allow message relaying* option in Relay Control 432 for those aliases.

Fully qualified aliases (no wildcards) are allowed to be list members
Click this checkbox if you want to allow aliases to be members of MDaemon mailing lists. Only actual accounts can be list members if this control is not enabled. **Note:** aliases containing wildcards are not permitted to be list members even if this option is enabled.

Mail from 'Postmaster,' 'abuse,' 'webmaster' requires authentication
When this option is enabled, MDaemon will require messages claiming to be from any of your "postmaster@...", "abuse@..." or "webmaster@..." aliases or accounts to be authenticated before MDaemon will accept them. Spammers and hackers know that these addresses might exist, and may therefore attempt to use one of them to send

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

mail through your system. This option will prevent them and other unauthorized users from being able to do so. For your convenience this option is also available on the SMTP Authentication 442 screen, located at: Security » Security Settings. Changing the setting here will change it there as well.

IP Shield honors aliases
By default the IP Shield 440 will honor aliases when checking incoming messages for valid domain/IP pairs. The IP Shield will translate an alias to the true account to which it points and thus honor it if it passes the shield. If you clear this checkbox then the IP Shield will treat each alias as if it is an address independent of the account that it represents. Thus, if an alias' IP address violates an IP Shield then the message will be refused. This option is mirrored on the IP Shield screen — changing the setting here will be change it there as well.

Replicate aliases to LDAP address book
Click this check box if you want aliases to be replicated to the LDAP address book. Alias replication is necessary for the LDAP remote verification feature to work reliably, but if you are not using that feature then replicating aliases to the LDAP address book is unnecessary. If you are not using remote verification then you can safely disable this feature to save processing time. For more information on remote LDAP verification, see: LDAP 106.

Aliases processing stops when result matches an existing account or list
When this option is enabled, alias processing will stop when the recipient of the incoming message matches an existing account or mailing list. This typically applies to aliases that include a wildcard. For example, if you have an alias set to, "`*@example.com=user1@example.com`," then this option will cause that alias to be applied only to addresses that do not actually exist on your server. So, if you also have the account, "`user2@example.com`," then messages addressed to user2 would still be delivered to him because the alias wouldn't be applied to those messages. But messages addressed to some non-existent account or list would be sent to "`user1@example.com`" because the wildcard alias would be applied to those messages. This option is enabled by default.

This option must be enabled when you are using Subaddressing 574, to avoid potential problems with handling those messages.

Use recursive aliasing
Click this check box if you want to process aliases recursively. Any alias match causes the resulting value to be reprocessed back through the entire alias list—it is possible to nest aliases up to 10 levels deep. For example, you could set up something like this:

```
user2@example.com = user1@example.com
user1@example.com = user5@example.net
user5@example.net = user9@example.org
```

This is logically identical to the single alias:

```
user2@example.com = user9example.org
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

It also means that:

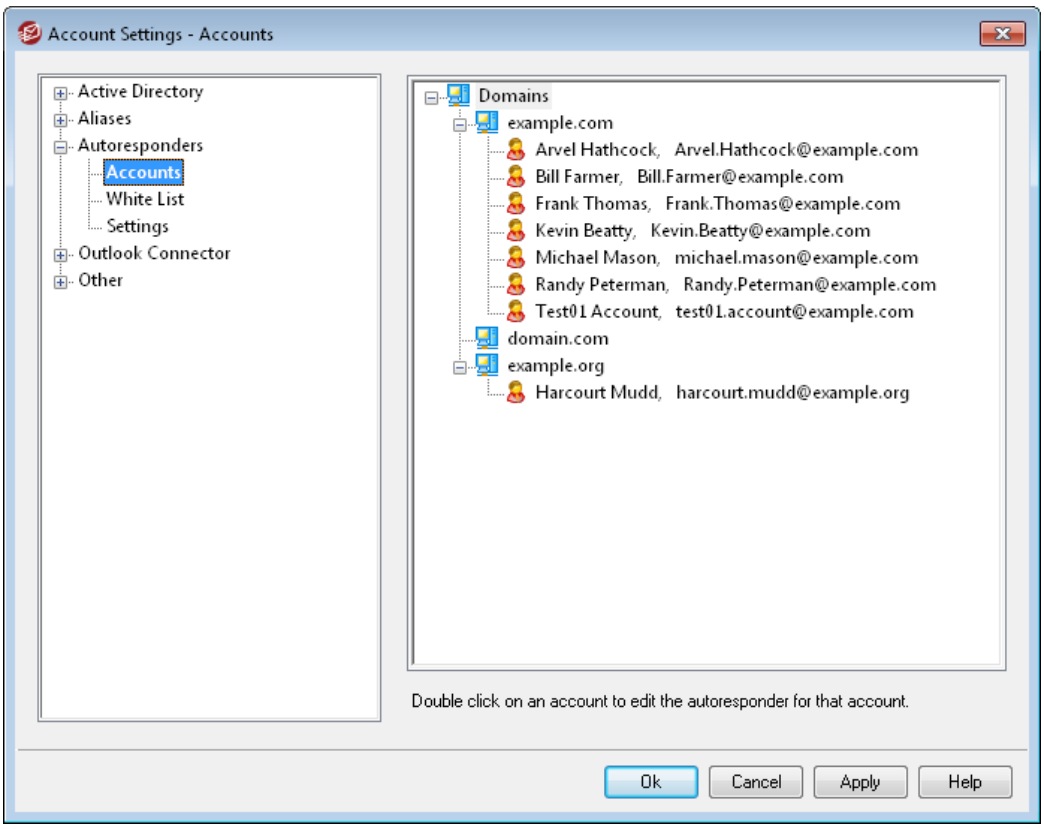
```
user1@example.com = user9example.org
```

See:

Aliases 613

5.3.3 Autoresponders

5.3.3.1 Accounts



Autoresponders are useful tools for causing incoming email messages to trigger certain events automatically, such as running a program, adding the sender to a mailing list, responding with an automatically generated message, and more. The most common use of autoresponders is to reply to incoming messages automatically with a user-defined message stating that the recipient is on vacation, is unavailable, will reply as soon as possible, or the like. MDaemon users with Web Access 526 to WorldClient 224 or Remote Administration 251 can use the options provided to compose auto response messages for themselves and schedule the dates they will be in use. Further, accounts with BlackBerry devices activated on MDaemon's BlackBerry Enterprise Server 314 can use the "Out of Office Reply" option under their device's email settings to configure their autoresponder. Finally, automated response messages are based on response scripts (`*.RSP` files), which support a large number of macros. These macros can be used to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

cause much of the script's content to be generated dynamically, making autoresponders quite versatile.

Auto response events are always honored when the triggering message is from a remote source. However, for messages originating locally, autoresponders will only be triggered if you enable the *Autoresponders are triggered by intra-domain mail* option, located on the Autoresponders » Settings 620 screen. You can also use an option on that screen to limit auto response messages to one response per sender per day.

Account List

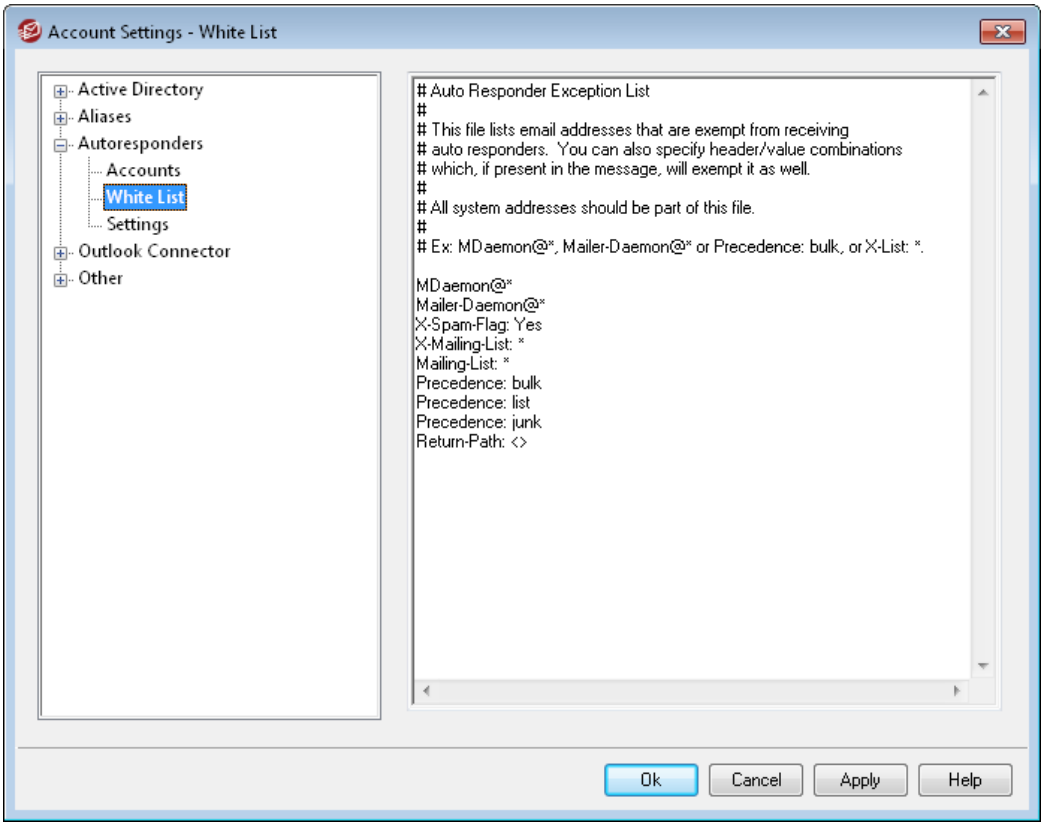
This area lists all available local mailboxes that can host an autoresponder. Double-click an account in this list to open its corresponding Autoresponder 529 screen, which is used to configure an autoresponder for that account.

See:

Autoresponders » White List 619
Autoresponders » Settings 620
Creating Auto Response Scripts 621
Account Editor » Autoresponders 529

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.3.3.2 White List



Use Autoresponder » White List to configure global exceptions to autoresponders. Messages from entries in this list will not receive any autoresponders. Both email addresses and header/value pairs can be included in the list. Enter one address or header/value pair per line. Wildcards are permitted.

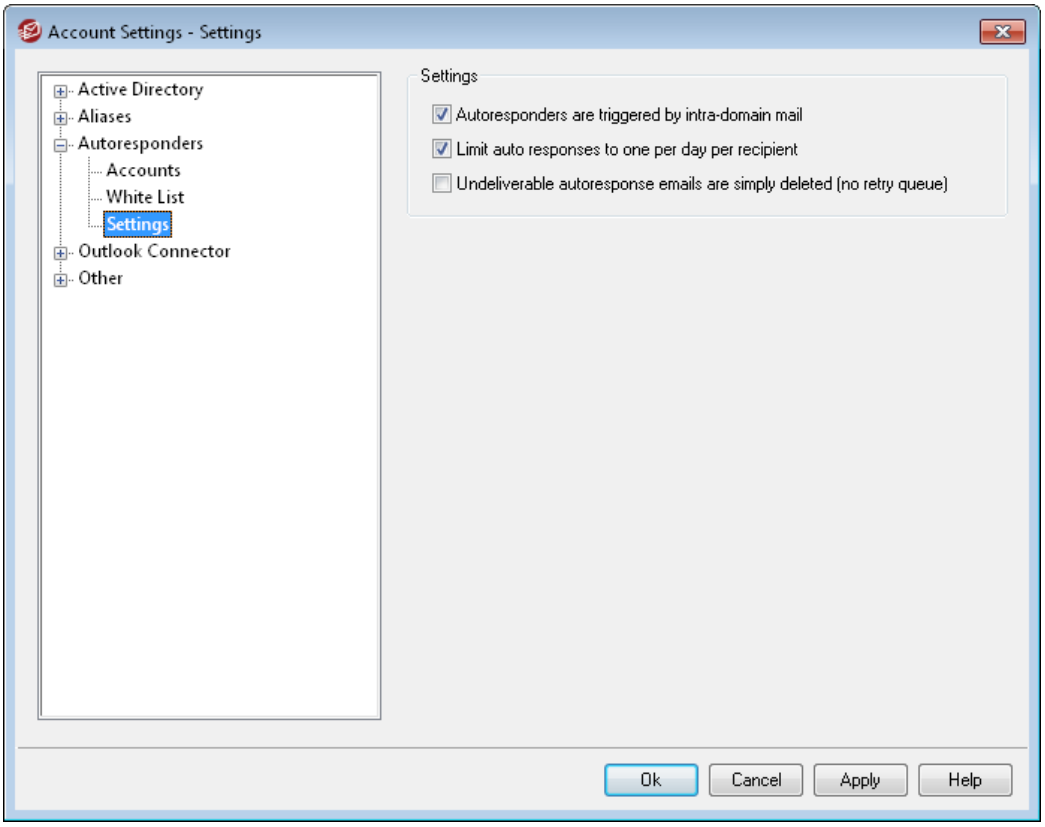
All system addresses (i.e. mdaemon@*, mailer-daemon@*, and so on) should be listed to help prevent mail loops and other problems.

See:

Autoresponders » Accounts 617
Autoresponders » Settings 620
Creating Auto Response Scripts 621
Account Editor » Autoresponders 529

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.3.3.3 Settings



Settings

Autoresponders are triggered by intra-domain mail
By default, both local and remote mail will trigger autoresponders. Clear this box if you do not wish mail that is sent from one local MDaemon domain to another to trigger them.

Limit auto responses to one per day per recipient
By default, autoresponders will only generate one response message per day for any given address. This prevents people from receiving the same redundant auto response message from you over and over again on the same day, every time they send you an email. Clear this box if you wish to send auto response messages each time someone sends you a message, even if they have already received one that day.

This option also helps to prevent message loops, which can occur when your auto response message is returned to an address that also has an autoresponder active. Instead of allowing both addresses to send auto response messages constantly back and forth to each other, this option would allow only one message to be sent to that address per day.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Undeliverable autoresponse emails are simply deleted (no retry queue)
Enable this option if you wish to delete undeliverable autoresponse messages when they expire from the remote queue, rather than move them into the retry queue 654 system.

See:

Autoresponders » Accounts 617
Autoresponders » White List 619
Creating Auto Response Scripts 621
Account Editor » Autoresponders 529

5.3.3.4 Creating Auto Response Scripts

Auto response scripts are text files that define the messages that are returned as the result of an autoresponder. These scripts are constructed as plain ASCII text files ending with the "`*.rsp`" file extension. When an auto response script is triggered by an autoresponder, the script file is processed and scanned for macros, which will then be replaced by actual data from the incoming message that triggered the response. Lines beginning with the "`#`" character are ignored and are used for comments.

There are several samples of scripts listed below, and there are several generic "`*.rsp`" files provided for you in MDaemon's `\app\` folder.

Auto Response Script Macros

`$HEADERS$` This macro will be replaced by all of the incoming message's headers. Text immediately preceding this macro will be duplicated at the start of each expanded line.

`$HEADER:XX$` This macro will cause the value of the header specified in place of "`xx`" to be expanded in the message. For example: If the incoming message has "`TO: joe@example.com`" then the `$HEADER:TO$` macro will expand to "`joe@example.com`". If the original message has "`SUBJECT: This is the subject`" then the `$HEADER:SUBJECT$` macro would be replaced with the text "`This is the subject`".

`$BODY$` This macro will be replaced by the entire message body. In an attempt to preserve character sets for different languages, MDaemon will read the message body as binary data rather than pure text, thus allowing a byte-for-byte copy of the message body.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

$BODY-AS-TEXT$	Like the $BODY$ macro, this macro will be replaced by the entire message body, but as text rather than binary. Text immediately preceding this macro will be duplicated at the start of each expanded line. So, using ">>$BODY-AS-TEXT$" in a script would place each line of the original message into the generated message, but each line would begin with ">>". Text can also be added to the right of this macro.
$SENDER$	This macro resolves to the full address contained in the incoming message's "From:" header.
$SENDERMAILBOX$	This macro resolves to the mailbox of the sender. The mailbox is the portion of the email address to the left of the "@" symbol.
$SENDERDOMAIN$	This macro resolves to the domain of the sender. This is the portion of the email address to the right of the "@" symbol.
$RECIPIENT$	This macro resolves to the full address of the message recipient.
$RECIPIENTMAILBOX$	This macro resolves to the mailbox of the message recipient. The mailbox is the portion of the email address to the left of the "@" symbol.
$RECIPIENTDOMAIN$	This macro resolves to the domain of the message recipient. The domain is the portion of the email address to the right of the "@" symbol.
$SUBJECT$	This macro resolves to the value of the "Subject:" header.
$MESSAGEID$	This macro resolves to the value of the "Message-ID" header.
$CONTENTTYPE$	This macro resolves to the value of the "Content-Type" header.
$PARTBOUNDARY$	This macro resolves to the value of the MIME "Part-Boundary" value found in the "Content-Type" header for multipart messages.
$DATESTAMP$	This macro expands to an RFC-2822 style date-time stamp line.
$ACTUALTO$	Some messages may contain an "ActualTo" field which generally represents the destination mailbox and host as it was entered by the original user prior

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

to any reformatting or alias translation. This macro expands to that value.

$ACTUALFROM$ Some messages may contain an "ActualFrom" field which generally represents the origination mailbox and host prior to any reformatting or alias translation. This macro expands to that value.

$REPLYTO$ This macro resolves to the value found in the "ReplyTo" header.

$PRODUCTID$ This macro expands to the MDaemon version information string.

AR_START Returns the auto-responder start date/time.

AR_END Returns the auto-responder end date/time.

Header Replacement Macros

The macros listed below control the auto response message's headers.

%SetSender%
ex: %SetSender%=mailbox@example.com
Just for the purpose of the auto-response message, this macro resets the sender of the original message before constructing the auto-response message headers. Thus, this macro controls the auto-response message's TO header. For example, if the sender of the original message were "user2@example.org" and recipient's autoresponder used the %SetSender% macro to change it to "user1@example.com" then the auto-response message's TO header would be set to "user1@example.com."

%SetRecipient%
ex: %SetRecipient%=mailbox@example.com
Just for the purpose of the auto-response message, this macro resets the recipient of the original message before constructing the auto-response message headers. Thus, this macro controls the auto-response message's FROM header. For example, if the recipient of the original message were "michael@example.com" and Michael's account had an autoresponder using the %SetRecipient% macro to change it to "michael.mason@example.com," then the auto-response message's FROM header would be set to "michael.mason@example.com."

%SetReplyTo%
ex: %SetReplyTo%=mailbox@example.com
Controls the value of the auto-response message's ReplyTo header.

%SetActualTo%
ex: %SetActualTo%=mailbox@example.com
Sets who the "actual" recipient of the message will be.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

%SetSubject%
ex: %SetSubject%=Subject Text
Replaces the value of the original message's subject.

%SetMessageId%
ex: %SetMessageId%=ID String
Changes the ID string of the message.

%SetPartBoundary%
ex: %SetPartBoundary%=Boundary String
Changes the part boundary.

%SetContentType%
ex: %SetContentType%=MIME type
Changes the content-type of the message to the declared value.

%SetAttachment%
ex: %SetAttachment%=filespec
Forces MDaemon to attach the specified file to the newly generated auto-response message.

5.3.3.4.1 Auto Response Script Samples

A simple auto response script, using several auto response script macros, might be called VACATION.RSP and look like this:

```
Greetings $SENDER$

You're message regarding '$SUBJECT$' won't be read by me because I'm
on vacation. Hurray!!!
Yours truly,

$RECIPIENT$
```

You can also use some of the header replacement macros to expand this script and control the headers that will be generated when the auto response message is mailed back to $SENDER$:

```
Greetings $SENDER$

You're message regarding '$SUBJECT$' won't be read by me because I'm
on vacation. Hurray!!!
Yours truly,

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\photos\me_on_vaction.jpg
```

Using that script the auto response message will have "RE: " added to the beginning of the subject and have the specified file attached.

The "%SetSubject%=RE: $SUBJECT$" line is handled like this:

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

1. The `$SUBJECT$` portion is expanded and replaced by the original message's subject text. This makes the string equivalent to:

   ```
   %SetSubject%=RE: Original Subject Text
   ```

2. MDaemon replaces the original subject, which it has stored in its internal buffers, with this newly calculated one. From that point forward, any use of "`$SUBJECT$`" in the script will return the new result.

Note the placement of the new macros - they are listed at the bottom of the response script. This is needed to avoid side effects. For example, if the `%SetSubject%` macro were placed before the `$SUBJECT$` macro, which appears in the second line of the response script, the subject text would have already been changed by the time the `$SUBJECT$` macro was expanded. Therefore, instead of replacing `$SUBJECT$` with the content of the original message's "`Subject:`" header, it would be replaced with whatever you have set the value of `%SetSubject%` to be.

See:

Autoresponders » Accounts 617
Autoresponders » White List 619
Autoresponders » Settings 620
Account Editor » Autoresponders 529

5.3.4 Outlook Connector for MDaemon

MDaemon PRO supports *Outlook Connector for MDaemon*, a separately licensed product available from Alt-N Technologies. Outlook Connector makes it possible for you to share your Microsoft Outlook calendars, contacts, tasks, and more with other MDaemon users, all without requiring Microsoft Exchange Server. Outlook Connector for MDaemon can effectively eliminate your dependency on Exchange.

When you have installed Outlook Connector for MDaemon, the Outlook Connector screens will be available from MDaemon's menu bar, located at: Accounts » Account Settings » Outlook Connector. This dialog is used for activating and configuring Outlook Connector and for authorizing specific accounts to use it.

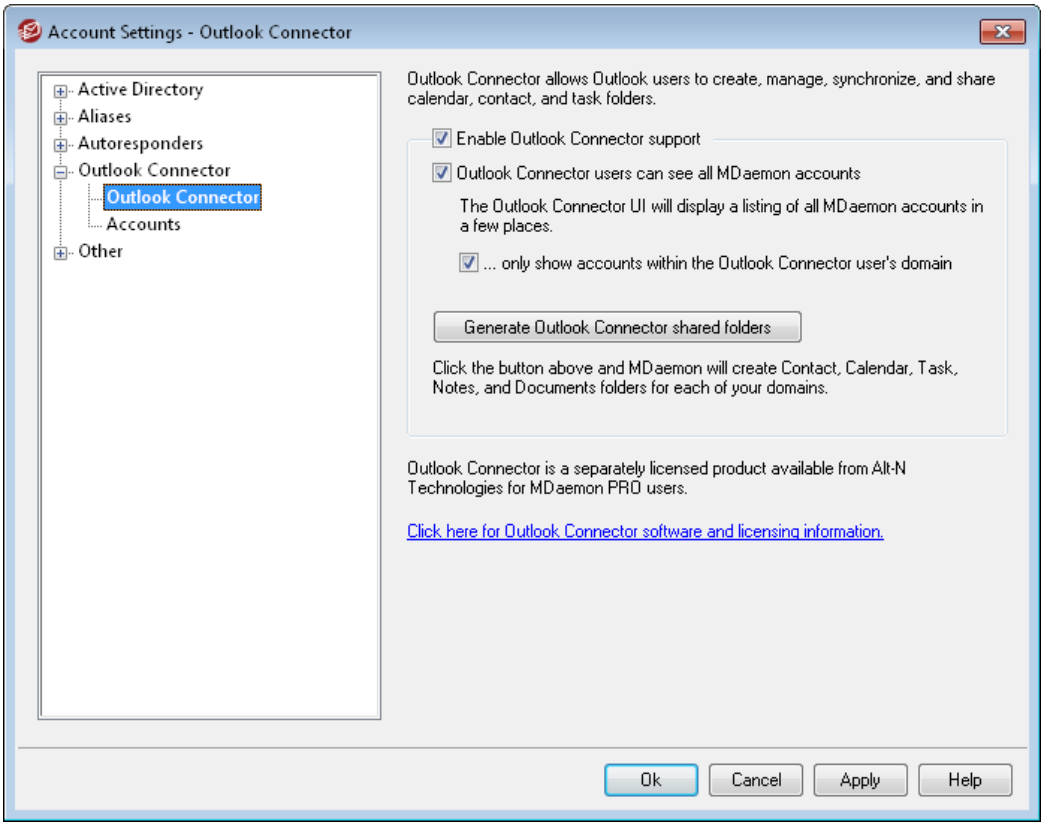
For more information, or to obtain Outlook Connector, visit the Outlook Connector for MDaemon page at www.altn.com.

See:

Outlook Connector 626
Outlook Connector Accounts 627

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.3.4.1 Outlook Connector


Account Settings - Outlook Connector
Active Directory
Aliases
Autoresponders
Outlook Connector
Outlook Connector
Accounts
Other
Outlook Connector allows Outlook users to create, manage, synchronize, and share calendar, contact, and task folders.
Enable Outlook Connector support
Outlook Connector users can see all MDaemon accounts
The Outlook Connector UI will display a listing of all MDaemon accounts in a few places.
... only show accounts within the Outlook Connector user's domain
Generate Outlook Connector shared folders
Click the button above and MDaemon will create Contact, Calendar, Task, Notes, and Documents folders for each of your domains.
Outlook Connector is a separately licensed product available from Alt-N Technologies for MDaemon PRO users.
Click here for Outlook Connector software and licensing information.
Ok
Cancel
Apply
Help

Outlook Connector

Enable Outlook Connector support
Click this checkbox to activate Outlook Connector for MDaemon. Your users will not be able to utilize Outlook Connector's features unless this option is enabled.

Outlook Connector users can see all MDaemon accounts
Click this option if you want all MDaemon accounts that have been authorized to connect via Outlook Connector to be visible on the *Permissions* list that appears in the Outlook Connector for MDaemon Plug-in. Outlook Connector users will choose the accounts from the list whom they wish to grant permission to share their Outlook items. When this feature in disabled, the Outlook Connector Plug-in's *Permissions* list will be blank and the users will have to enter email addresses manually. Only addresses belonging to accounts authorized to connect via Outlook Connector will be able to share the Outlook items. If a user enters an address that is not authorized then the items will simply not be shared with that address unless it is authorized to connect via Outlook Connector at some later time.

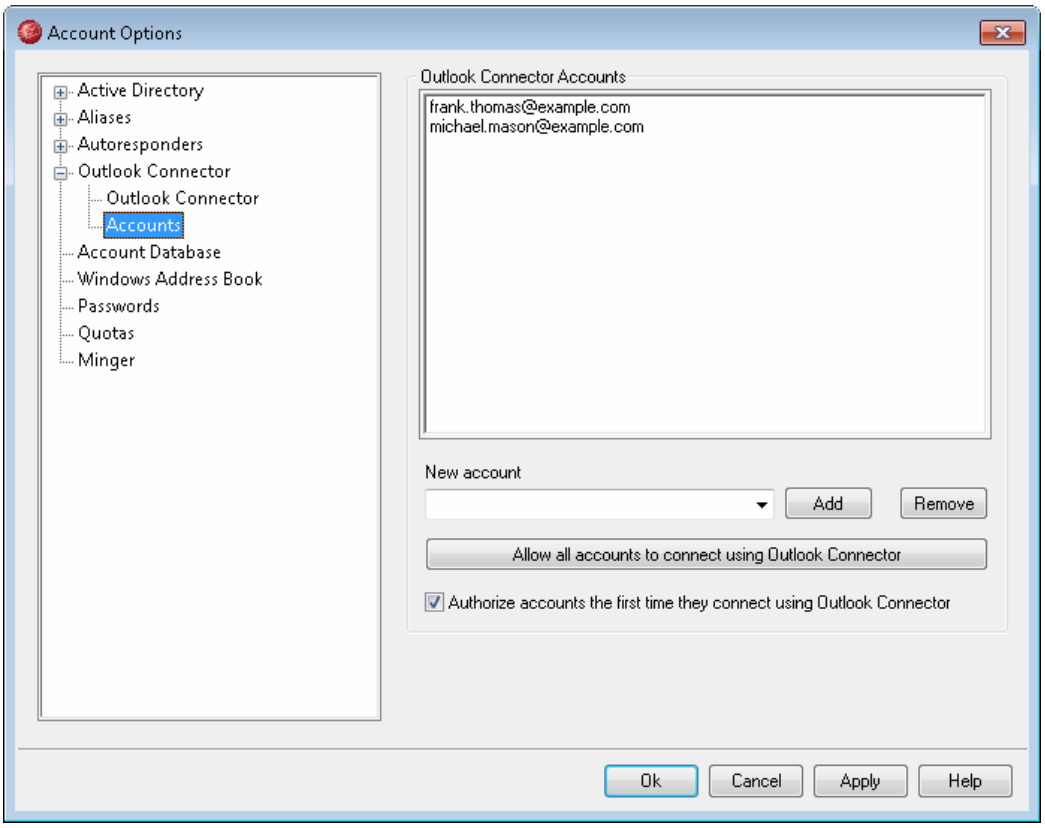
...only show accounts within the Outlook Connector user's domain
This option is only available when the *Outlook Connector users can see all MDaemon accounts* option above is enabled. Click this checkbox if you want only users who are authorized to connect via Outlook Connector, and who belong to same domain, to appear on the *Permissions* list in the Outlook Connector Plug-in. Accounts belonging to different domains will not be listed even if they are

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

authorized to connect via Outlook Connector.

Generate Outlook Connector shared folders
Click this button to generate a set of Outlook Connector folders for each domain. It will generate the following folders: Contacts, Appointment, Journal, Tasks, and Notes.

5.3.4.2 Accounts



Outlook Connector Accounts

This is the list of MDaemon accounts who are authorized to share their Outlook folders, Calendars, Contacts, Notes, and so on via Outlook Connector. You can add accounts to the list by using the options outlined below.

New account
To add an MDaemon account to the list of authorized Outlook Connector Accounts, select the desired account from this drop-down list and then click *Add*. To remove an account, select the account and then click *Remove*.

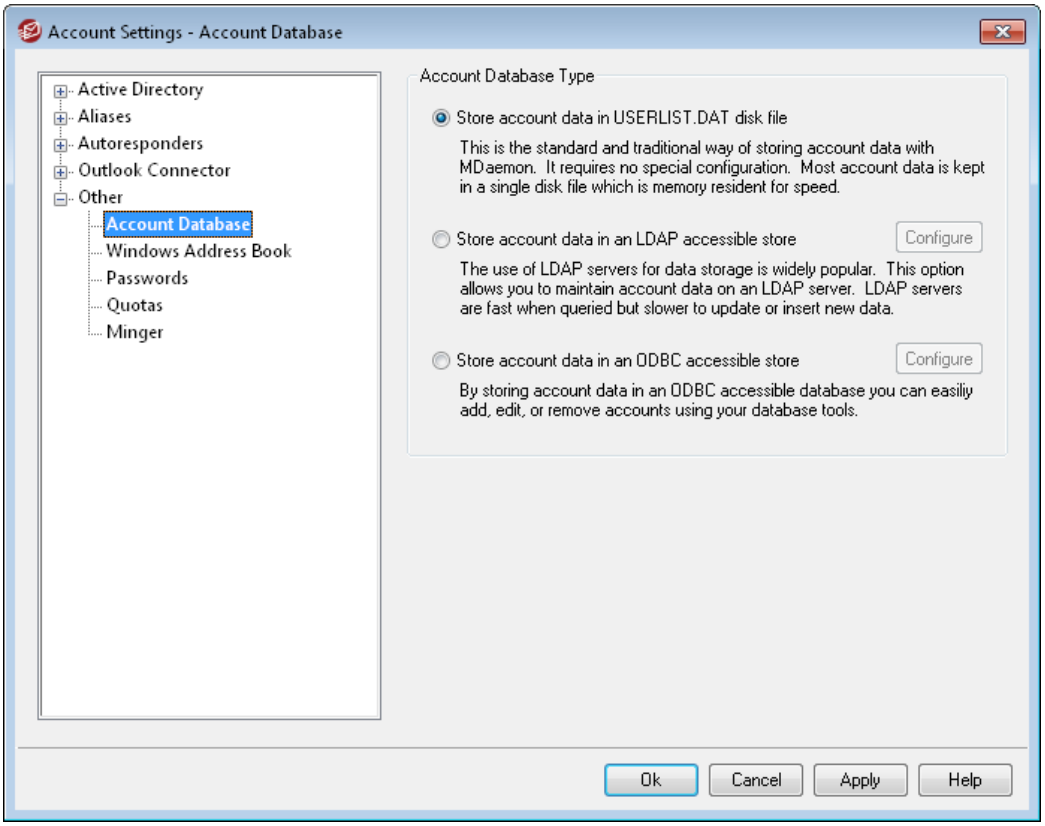
Allow all accounts to connect using Outlook Connector
To instantly authorize all MDaemon accounts to connect via Outlook Connector, click this button and all MDaemon accounts will be added to the *Outlook Connector*

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Users list.

Authorize accounts the first time they connect using Outlook Connector
Click this checkbox if you want individual accounts to be added to the *Outlook Connector Accounts* list the first time each connects using Outlook Connector. **Note:** if you enable this option then you have in effect authorized all MDaemon accounts to use Outlook Connector for MDaemon. The accounts simply will not be added to the list until the first time each one uses it.

5.3.5 Account Database


Account Settings - Account Database
Active Directory
Aliases
Autoresponders
Outlook Connector
Other
Account Database
Windows Address Book
Passwords
Quotas
Minger
Account Database Type
Store account data in USERLIST.DAT disk file
This is the standard and traditional way of storing account data with MDaemon. It requires no special configuration. Most account data is kept in a single disk file which is memory resident for speed.
Store account data in an LDAP accessible store
Configure
The use of LDAP servers for data storage is widely popular. This option allows you to maintain account data on an LDAP server. LDAP servers are fast when queried but slower to update or insert new data.
Store account data in an ODBC accessible store
Configure
By storing account data in an ODBC accessible database you can easily add, edit, or remove accounts using your database tools.
Ok
Cancel
Apply
Help

The Account Database dialog (located under Accounts » Account Settings) is used to designate the method that you want MDaemon to use to maintain your user accounts: ODBC, LDAP, or the local USERLIST.DAT system.

Account Database Type

Store account data in USERLIST.DAT disk file
Choose this option if you want MDaemon to use its internal USERLIST.DAT file as the account database. This is MDaemon's default setting and causes all of the MDaemon user account information to be stored locally. Most information is stored in a single file, which is memory resident to increase efficiency and speed.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Store account data in LDAP accessible store
Choose this option if you want MDaemon to use your LDAP server as the MDaemon user database rather than ODBC or its local `USERLIST.DAT` system. You might want to use this method of maintaining your user account data if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally. LDAP servers typically respond quickly and efficiently to queries but are slower to update or insert new data.

Configure
When the LDAP account data option is selected, click this button to open the LDAP screen 106 for configuring your LDAP server settings.

Store account data in an ODBC accessible store
Choose this option if you want to use an ODBC compliant database as your MDaemon account database.

Configure
When the ODBC account data option is selected, click this button to open the ODBC Selector Wizard 629 for selecting and configuring your ODBC compliant database.

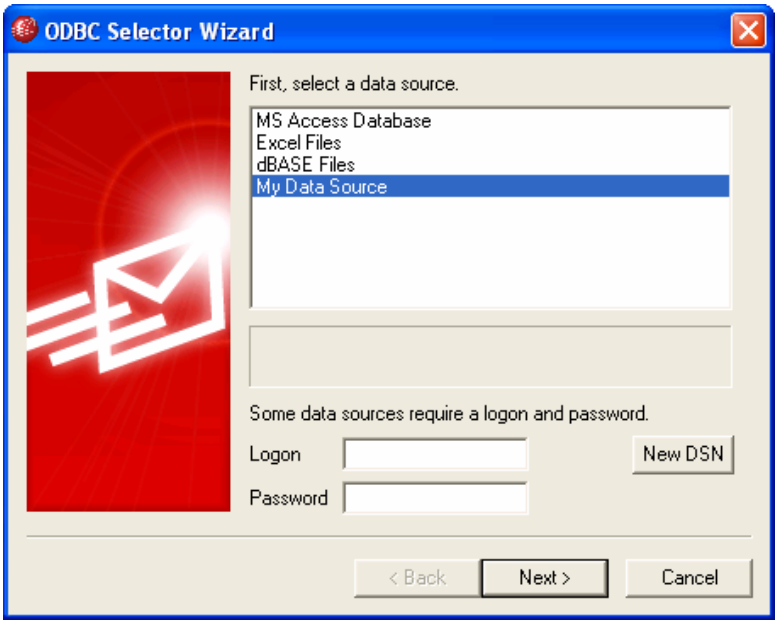
5.3.5.1 ODBC Selector Wizard

Use the ODBC Selector Wizard to select or configure an ODBC compliant data source to use as your MDaemon account database.

Migrating Your Account Database to an ODBC Accessible Store

1. On the Account Database dialog (`Accounts » Account Settings » Account Database`), click **Store account data in an ODBC accessible store**, and then click **Configure** to open the ODBC Selector Wizard.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

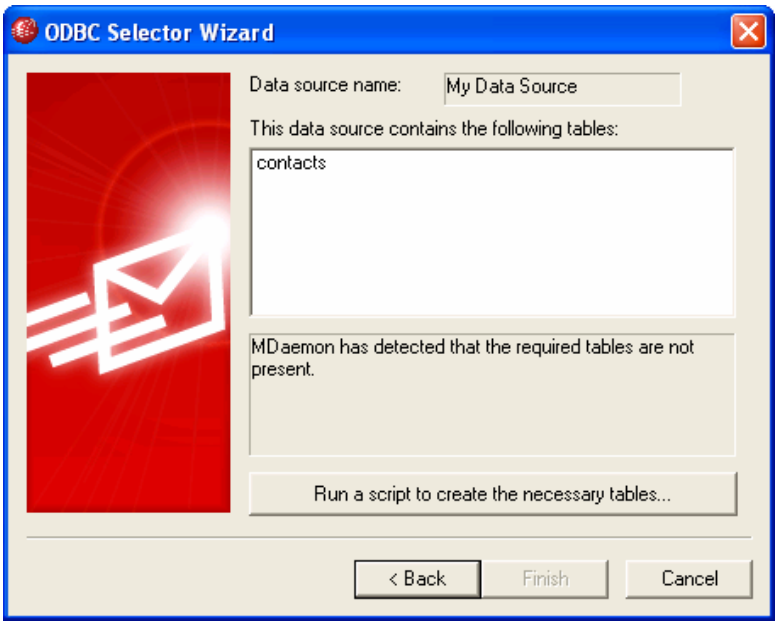


2. Select the **data source** that you wish to use for your account database. If there is not a compatible data source listed, click **New DSN** and then follow the instructions listed under, **Creating a New ODBC Data Source** 631.

3. If required, enter the data source's **Logon** and **Password**.

4. Click **Next**.

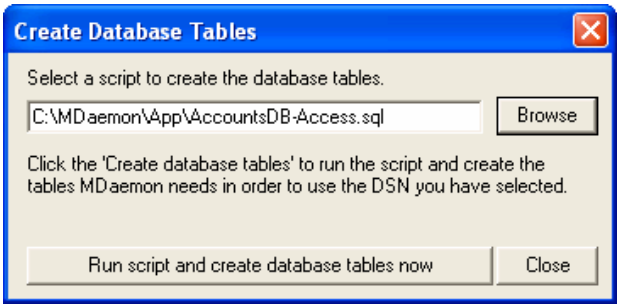
5. If the data source already contains the tables that are required by MDaemon, go to **Step 8**. Otherwise, click **Run a script to create the necessary tables...**



6. Type the file path (or **Browse**) to the desired script file that you wish to use to

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

create the tables for your database application. The \MDaemon\app\ folder contains scripts for several of the most popular database applications.


Create Database Tables
Select a script to create the database tables.
C:\MDaemon\App\AccountsDB-Access.sql
Browse
Click the 'Create database tables' to run the script and create the tables MDaemon needs in order to use the DSN you have selected.
Run script and create database tables now
Close

7. Click **Run script and create database tables now**, Click **OK**, and click **Close**.
8. Click **Finish**, and click **OK** to close the Account Database dialog.
9. A database migration tool will migrate all of your user accounts to the ODBC data source and then close MDaemon. Click **OK**, and then restart MDaemon and begin using the new ODBC account database.

See:

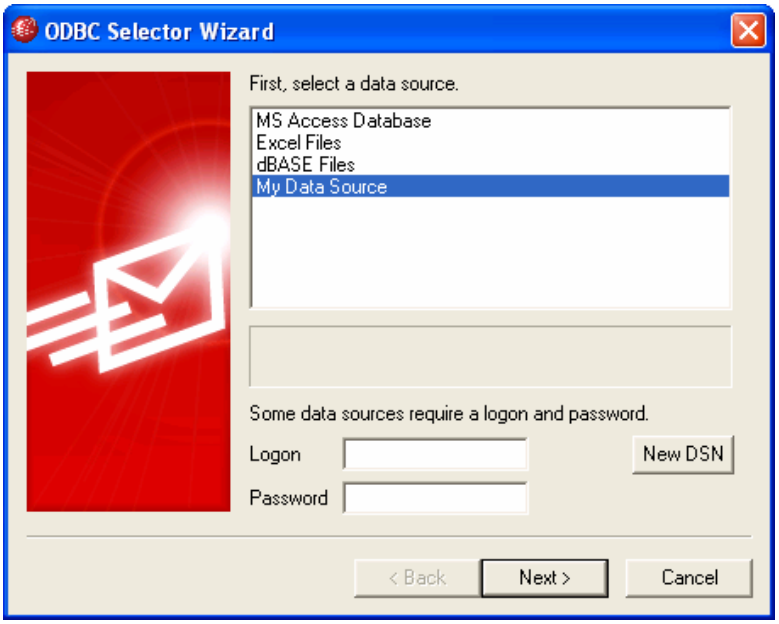
Account Database 628
Creating a New ODBC Data Source 631

5.3.5.1.1 Creating a New Data Source

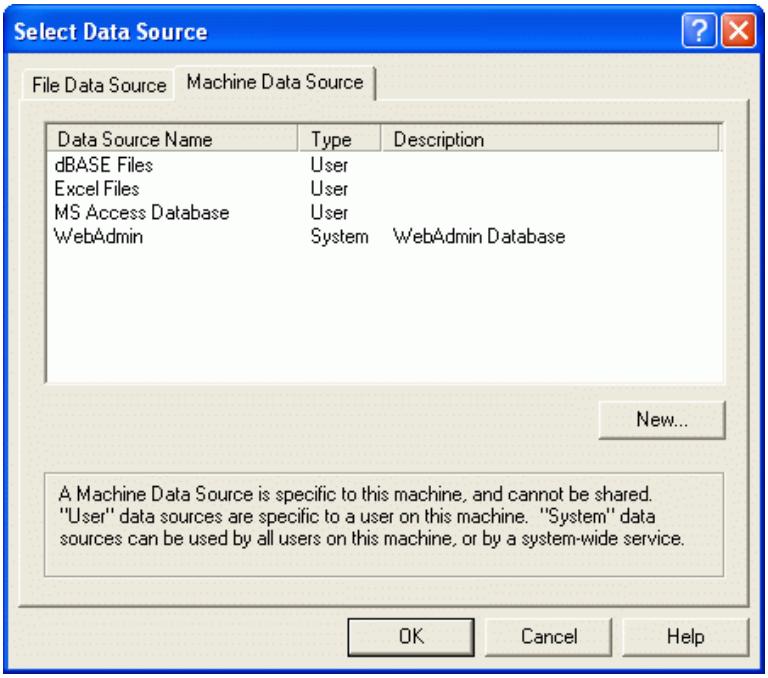
To create a new ODBC data source:

1. On the Account Database dialog (Accounts » Account Settings » Account Database), click **Store account data in an ODBC accessible store**, and then click **Configure** to open the ODBC Selector Wizard.
2. Click **New DSN** to open the Select Data Source dialog.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

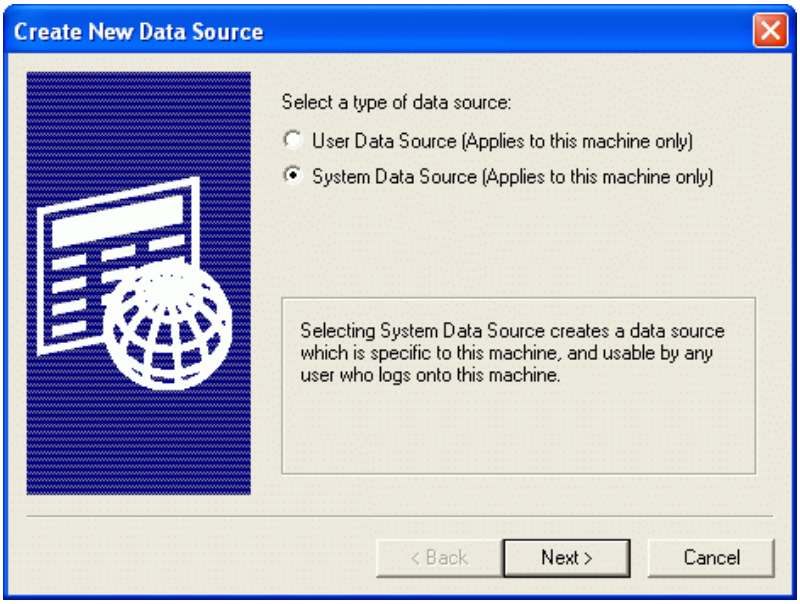


3. Switch to the **Machine Data Source** tab, and click **New...** to open the Create New Data Source dialog.

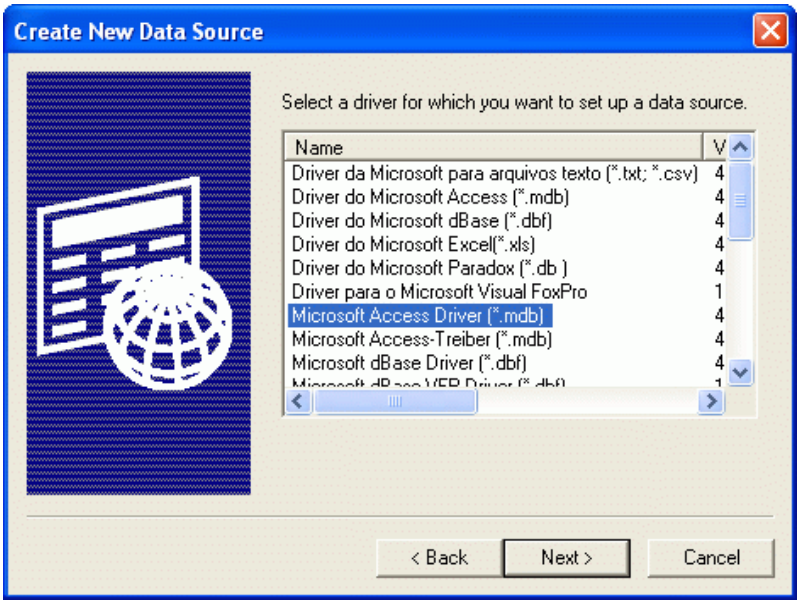


4. Select **System Data Source**, and click **Next**.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

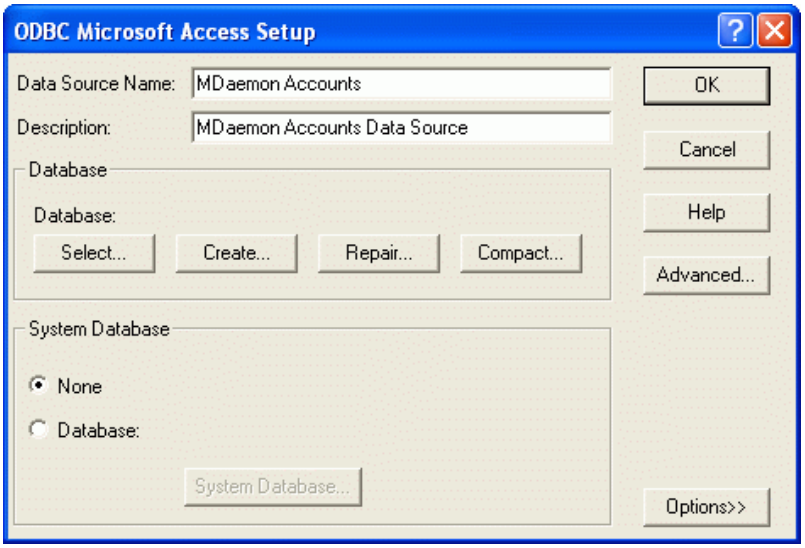

Create New Data Source
Select a type of data source:
User Data Source (Applies to this machine only)
System Data Source (Applies to this machine only)
Selecting System Data Source creates a data source which is specific to this machine, and usable by any user who logs onto this machine.
< Back
Next >
Cancel

5. Select the **database driver** for which you wish to set up the data source, and click **Next**.


Create New Data Source
Select a driver for which you want to set up a data source.
Name
Driver da Microsoft para arquivos texto (*.txt; *.csv)
Driver do Microsoft Access (*.mdb)
Driver do Microsoft dBase (*.dbf)
Driver do Microsoft Excel(*.xls)
Driver do Microsoft Paradox (*.db)
Driver para o Microsoft Visual FoxPro
Microsoft Access Driver (*.mdb)
Microsoft Access-Treiber (*.mdb)
Microsoft dBase Driver (*.dbf)
< Back
Next >
Cancel

6. Click **Finish** to display the driver-specific setup dialog. The appearance of this dialog will vary based on which driver you have selected (Microsoft Access Setup dialog shown below).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.



7. Designate a **Data Source Name** for your new data source and provide any other information required by the driver-specific dialog (such as creating or specifying a database, choosing a directory or server, and so on).

8. Click **OK** to close the driver-specific dialog.

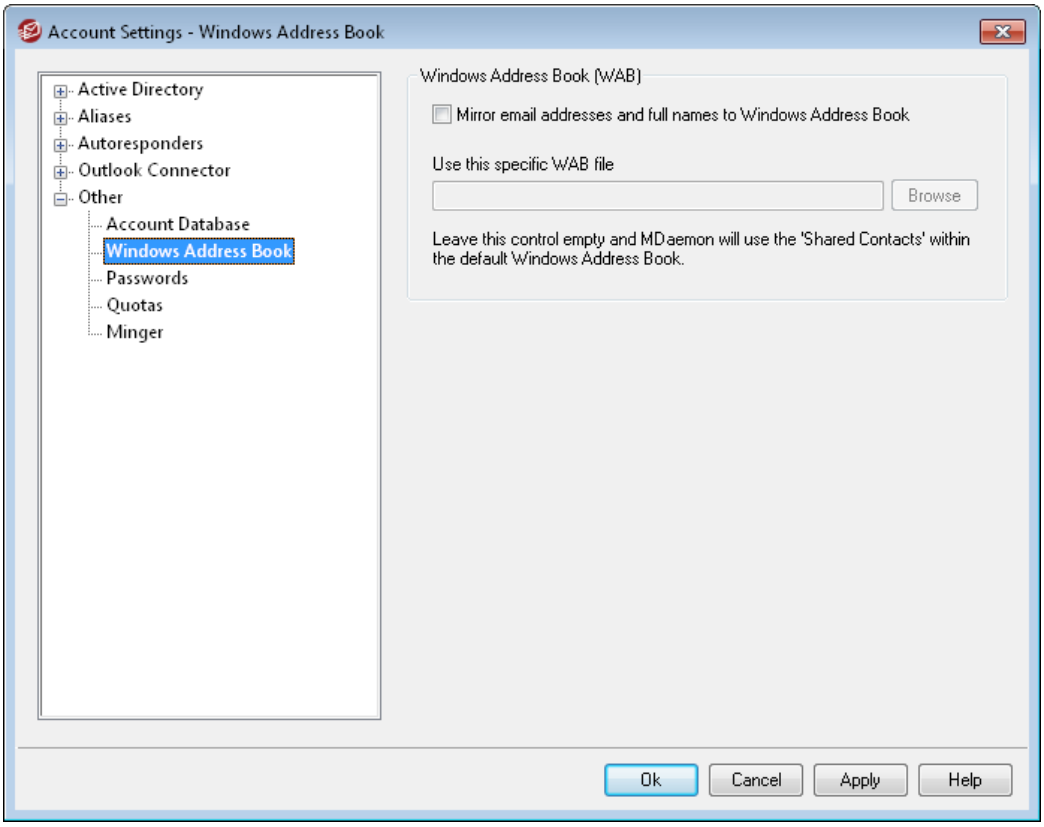
9. Click **OK** to close the Select Data Source dialog.

See:

Account Database 628
ODBC Selector Wizard - Account Database 629

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.3.6 Windows Address Book



MDaemon has the ability to automatically keep a Windows Address Book file (*.wab) or Microsoft Outlook Contact Store current with each account's full name and email address. This is desirable for those who wish to share an address book amongst users of products like Outlook, but do not wish to use an LDAP server or WorldClient Instant Messenger 225 for that purpose.

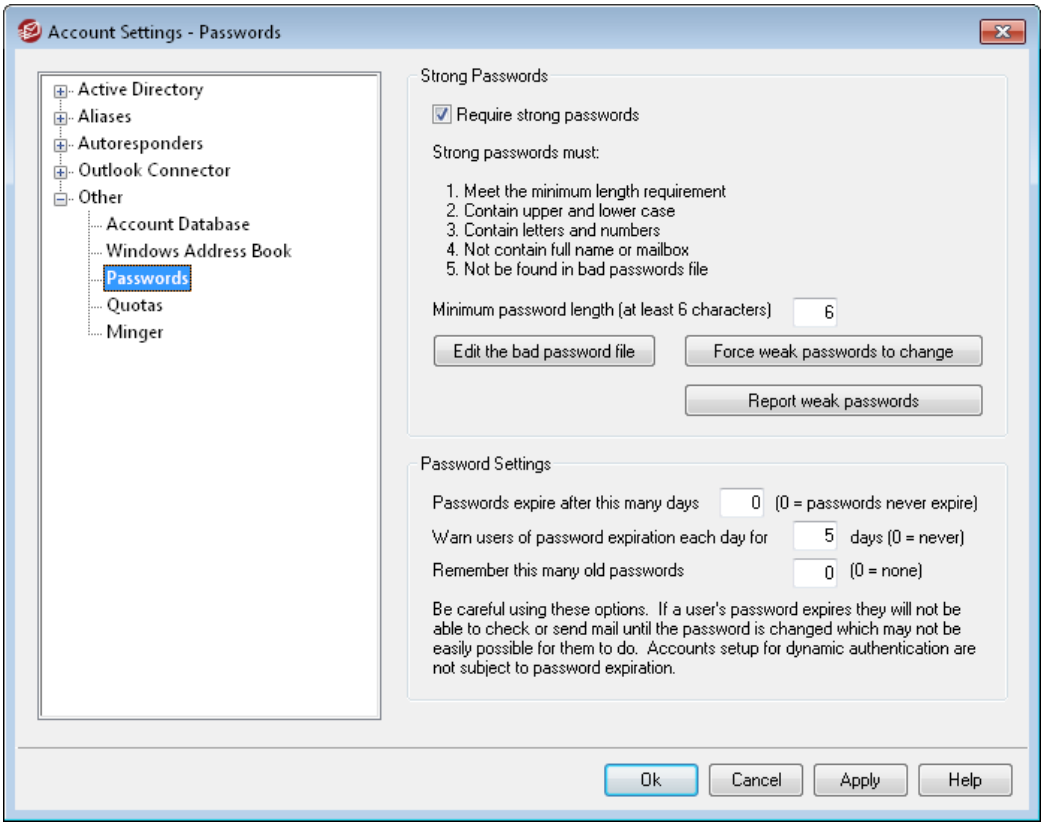
Windows Address Book (WAB)

Mirror email addresses and full names to Windows Address Book
Enable this checkbox if you want your users' names and email addresses to be mirrored to a `*.wab` file or the Microsoft Outlook Contact Store. In the Windows Address Book, on the Tools→Options menu, you can configure whether or not your Windows Address Book will share contact information between Outlook and other applications by storing data in the Microsoft Outlook Contact Store or an address book (`*.wab`) file.

Use this specific WAB file
Specify the path to the `*.wab` file in which you wish to mirror your user information. If you leave this control empty then MDaemon will use the shared contacts store within the default Windows Address Book.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.3.7 Passwords


Account Settings - Passwords
Active Directory
Aliases
Autoresponders
Outlook Connector
Other
Account Database
Windows Address Book
Passwords
Quotas
Minger
Strong Passwords
Require strong passwords
Strong passwords must:
1. Meet the minimum length requirement
2. Contain upper and lower case
3. Contain letters and numbers
4. Not contain full name or mailbox
5. Not be found in bad passwords file
Minimum password length (at least 6 characters) 6
Edit the bad password file
Force weak passwords to change
Report weak passwords
Password Settings
Passwords expire after this many days 0 (0 = passwords never expire)
Warn users of password expiration each day for 5 days (0 = never)
Remember this many old passwords 0 (0 = none)
Be careful using these options. If a user's password expires they will not be able to check or send mail until the password is changed which may not be easily possible for them to do. Accounts setup for dynamic authentication are not subject to password expiration.
Ok
Cancel
Apply
Help

Strong Passwords

Require strong passwords
By default, MDaemon requires strong passwords when creating new accounts or changing existing passwords. Clear this check box if you wish to disable the strong password requirement.

Strong passwords must:

- Meet the minimum length requirement.
- Contain upper and lower case letters.
- Contain letters and numbers.
- Not contain the user's full name or mailbox name.
- Not be found in the bad passwords file.

Minimum password length (at least 6 characters)
Use this option to set the minimum password length required for strong passwords. This must be set to at least 6 characters, but a higher value is recommended. Changing this setting does not automatically trigger a required password change for accounts with passwords shorter than the new minimum, but when those users next change their password this setting will be enforced.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Regardless of the minimum setting, passwords can be longer than 15 characters.

Edit the bad password file
Click this button to edit the bad password file. Entries listed in this file are case insensitive and cannot be used as passwords. If you wish to create more complex or versatile entries, you can use Regular Expressions 370 to do so. Entries beginning with "!" are treated as Regular Expressions.

Force weak passwords to change
Click this button if you wish to force all accounts with a weak password to change their passwords. This will lock out every account with a weak password until the password is changed. The password can be changed by an administrator via the MDaemon interface, or a locked out user can change the password via WorldClient or the remote administration interface. When the user attempts to log in using the old password, he or she will be required to create a new one before proceeding.

Report weak passwords
Click this button to generate a report of all MDaemon accounts with a weak password. The report will be emailed to whatever email address you specify after clicking OK.

Password Settings

Passwords expire after this many days (0=passwords never expire)
Use this option if you wish to set a maximum number of days that an account can be accessed before being required to change its password. The default value in this option is "0", which means that passwords never expire. But if you set it to, for example, 30 days then the user will have 30 days to change his or her password, starting from the last time the account was edited in the user interface or logged in to POP, IMAP, SMTP, or WorldClient. If a user's password is changed then that will reset the timer. If a user's password expires then he or she will not be able to access POP, IMAP, SMTP, WorldClient, or Remote Administration. The user can, however, still connect to WorldClient or Remote Administration where he or she will then be required to change the password before proceeding. Email clients such as Outlook, Thunderbird, and the like cannot be used to change the password. Further, many clients will not even show a helpful error message to users, therefore they may need administrator assistance to figure out why their login is failing.

In order for users to be able to change their passwords via WorldClient or Remote Administration they must first be granted the "...edit password" web access permission on the Web Services 587 screen. Further, because changing the password may not be easy or possible for some users, you should exercise caution before using this option.

Warn users of password expiration each day for [xx] days (0 = never)
Accounts with a password that is about to expire can receive a daily reminder email

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

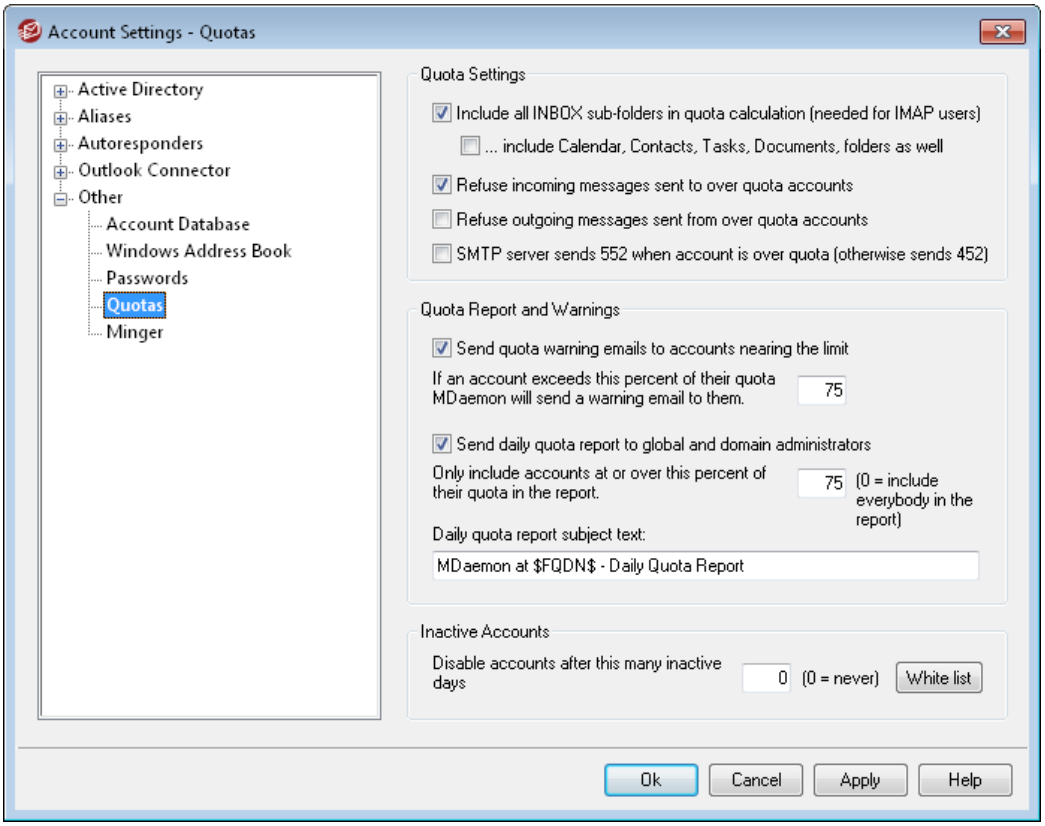
that the password needs to be changed. Use this option to designate the number of days before the password expires that you want MDaemon to start sending these daily emails.

Remember this many old passwords (0=none)
Use this option to specify the number of old passwords that you want MDaemon to remember for each user. When users change their passwords they will not be allowed to reuse old passwords. This option is set to "0" (disabled) by default.

See:

Account Editor » Account Details 521
Account Editor » Web Services 526
Regular Expressions 370

5.3.8 Quotas


Account Settings - Quotas
Active Directory
Aliases
Autoresponders
Outlook Connector
Other
Account Database
Windows Address Book
Passwords
Quotas
Minger
Quota Settings
Include all INBOX sub-folders in quota calculation (needed for IMAP users)
... include Calendar, Contacts, Tasks, Documents, folders as well
Refuse incoming messages sent to over quota accounts
Refuse outgoing messages sent from over quota accounts
SMTP server sends 552 when account is over quota (otherwise sends 452)
Quota Report and Warnings
Send quota warning emails to accounts nearing the limit
If an account exceeds this percent of their quota MDaemon will send a warning email to them.
75
Send daily quota report to global and domain administrators
Only include accounts at or over this percent of their quota in the report.
75
(0 = include everybody in the report)
Daily quota report subject text:
MDaemon at $FQDN$ - Daily Quota Report
Inactive Accounts
Disable accounts after this many inactive days
0
(0 = never)
White list
Ok
Cancel
Apply
Help

Quotas Settings

Include all INBOX sub-folders in quota calculation (needed for IMAP users)
When this box is checked, all message files in all sub-folders under a user's account will apply toward any size or message number limitations placed on that account. Otherwise, only actual message files in the inbox will count toward those limitations. This is generally only needed for IMAP users.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

...include Calendar, Contacts, Tasks, Documents, folders as well
Click this check box if you wish to include all calendar, contacts, tasks, and documents folders in the quota calculations.

Refuse incoming messages sent to over quota accounts
By default, when an account has a message quota restriction placed on it and the quota has been reached, MDaemon will no longer accept any incoming messages for the account until the account holder deletes some of his or her stored mail. Clear this checkbox if you do not wish to refuse incoming messages for over quota accounts.

Refuse outgoing messages sent from over quota accounts
Check this box if you wish to refuse outgoing messages sent from any account that has reached its quota. An over-quota account will no longer be able to send mail until some of its stored messages have been deleted. This option is disabled by default.

SMTP server sends 552 when account is over quota (otherwise sends 452)
By default, when an account is over quota 537 MDaemon sends the 452 error code (i.e "Requested action not taken: insufficient system storage") during the SMTP process. This code generally means that the server should try again later. Check this box if you wish to send the permanent failure 552 error code instead ("Requested mail action aborted: exceeded storage allocation").

Quota Report and Warnings

Send quota warning emails to accounts nearing the limit
When an MDaemon account exceeds this percentage value of either its *Maximum number of messages stored at once* or *Maximum disk space allowed* quota restriction designated on the Account Editor 537, a warning message will be sent to the account. This message will list the account's current number of stored messages, the size of its mailbox, and the percentage used and the percentage remaining. Further, if an existing warning is found in the account's mailbox it will be replaced with an updated message. Disable this option if you do not wish to send quota warning messages to users.

Send daily quota report to global and domain administrators
Check this box and specify a value if you wish to send a daily quota report to all global and domain administrators. The report will contain quota statistics for all users at or over the designated percentage of their quota restriction. Use "0" as the value if you want the report to include quota statistics on everyone.

Daily quota report subject text:
Use this option if you wish to customize the subject text of the daily quota report that MDaemon sends to the administrators. See `QuotaReport.dat` in the `MDaemon\APP` folder if you wish to customize the report itself.

Inactive Accounts

Disable accounts after this many inactive days XX (0=never)
Use this option if you wish to disable accounts automatically that have been

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

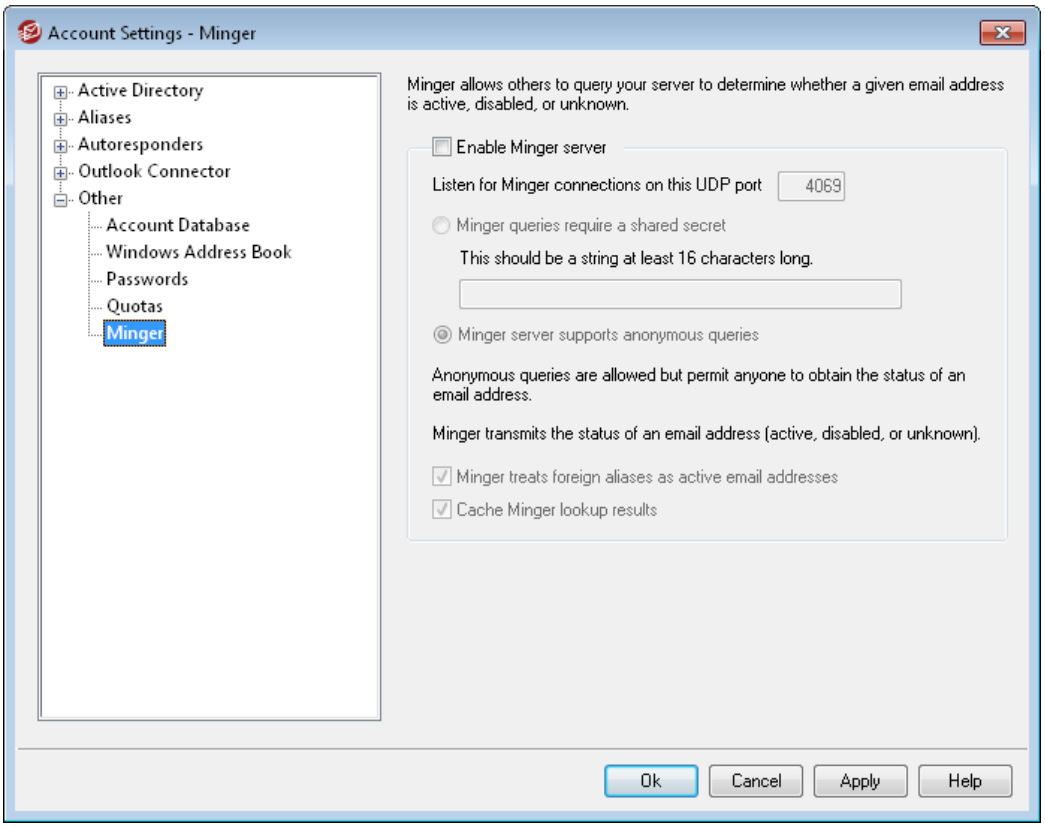
inactive for more than a specified number of days. Once the maximum number of inactive days has been reached, the account is disabled and an email is sent to the postmaster. Replying to the email will re-enable the account. Processing is done as part of the midnight cleanup event each night. The default is 0 (disabled).

White list
Accounts added to this white list are exempt from the inactive account disabling feature.

See:

Account Editor » Quotas 537
Template Manager » Quotas 596

5.3.9 Minger


Account Settings - Minger
Active Directory
Aliases
Autoresponders
Outlook Connector
Other
Account Database
Windows Address Book
Passwords
Quotas
Minger
Minger allows others to query your server to determine whether a given email address is active, disabled, or unknown.
Enable Minger server
Listen for Minger connections on this UDP port
4069
Minger queries require a shared secret
This should be a string at least 16 characters long.
Minger server supports anonymous queries
Anonymous queries are allowed but permit anyone to obtain the status of an email address.
Minger transmits the status of an email address (active, disabled, or unknown).
Minger treats foreign aliases as active email addresses
Cache Minger lookup results
Ok
Cancel
Apply
Help

Located under Accounts » Account Settings, Minger is an email address verification protocol created by Alt-N Technologies. Originally based loosely on the Finger protocol, Minger is primarily intended to provide a simple and efficient mechanism for allowing others to query your server in order to verify whether or not an email address is valid. For efficiency Minger uses UDP rather than TCP, and for security it can require authentication—though it supports anonymous queries as well. The Minger dialog is used to enable/disable MDaemon's Minger server, designate the port that it will use

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

(the default is 4069), and choose whether to require authentication via a shared secret system or to allow anonymous queries.

MDaemon also has a Minger client, which is built in to the Domain Gateways system (see Verification 170). Each domain for which MDaemon is acting as a gateway or backup server can be configured to use Minger so that MDaemon will connect to the remote server and verify whether or not the recipients of incoming messages for that domain are valid. This prevents you from having to assume that all recipients are valid addresses.

You can find the latest draft of the Minger protocol at:

http://tools.ietf.org/html/draft-hathcock-minger-06

Minger Server

Enable Minger server
Click this checkbox to enable MDaemon's Minger server.

Listen for Minger connections on this UDP port
This is the port on which the Minger server will listen for connections. The Internet Assigned Numbers Authority (IANA) has reserved and assigned TCP and UDP port 4069 for use with Minger clients and servers. Changing this port is not recommended as it has been reserved exclusively for Minger use.

Minger queries require a shared secret
If you wish to require authentication via a shared secret system, choose this option and enter a text string of at least 16 characters. When this option is chosen the Minger server will refuse unauthenticated queries.

Minger server supports anonymous queries
Choose this option if you wish to support anonymous Minger queries—the connecting client isn't required to authenticate itself before making address verification queries. This is similar to what can be accomplished now by sources using the `SMTP VRFY` command or SMTP "call back" or "call forward", but it is much more efficient and doesn't result in lots of dropped SMTP sessions over TCP, SMTP logs cluttered with dropped sessions, and similar problems inherent in those methods.

Minger treats foreign aliases as active email addresses
When this box is checked, Minger will treat foreign aliases (aliases that point to external addresses) as if they were active known addresses. Also, this behavior is forced when a query comes from SecurityGateway to MDaemon regardless of the state of this option's setting.

Cache Minger lookup results
By default MDaemon will cache Minger lookup results. If you do not wish to cache them, disable this option.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

5.4 Importing Accounts

5.4.1 Importing Accounts from a Text File

Click the Accounts » Importing... » Import accounts from a comma delimited text file... menu selection to access this account generation feature. It can also be reached by clicking the *Import* button on the Account Manager. This is a simple method for importing and automatically generating mail accounts. MDaemon will read a text file and generate new mail accounts using as little as just the first and last names of the user. If you are careful to setup your account template strings properly (see New Accounts Template 581) you can generate unique accounts using only the first and last names, but you can also include many other options for specific user settings if you want to override the new account defaults. All fields must be separated by commas.

Each line of the comma delimited text file must contain only a single user's entry. The first line must be a base line giving the names and sequence of the fields in subsequent lines. A sample file would look something like this:

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"michael", "Michael Mason", "C:\Mail\Michael\", N
```

The field names in the base line are used by MDaemon to determine the data sequence and can therefore appear in any order. Each of the field names must be in quotes.

All "String" values must be contained in quotes, and a "bool" field value is considered `FALSE` unless the first char is: `y`, `Y`, `1`, `t`, or `T`.

First, middle, and last names are acceptable in each full name. However, you may not use commas in them.

After running the import process, MDaemon will create `TXIMPORT.LOG`, detailing the import results and listing which accounts imported successfully and which failed. Typical reasons why an account might not be imported would include a conflict with an existing account's mailbox, name, or directory information, a conflict with an existing alias to an account, or a conflict with a mailing list name.

See the description of the `MD_ImportUserInfo()` and the `MD_ExportAllUsers()` within the `MD-API.HTML` file located in your `\API\` directory, for more information on the field mappings.

Use the following values in the base line to map to MDaemon account fields:

Field Name	Type
MailBox	string

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Domain	string
FullName	string
MailDir	string
Password	string
AutoDecode	bool
IsForwarding	bool
AllowAccess	bool
AllowChangeViaEmail	bool
KeepForwardedMail	bool
HideFromEveryone	bool
EncryptMail	bool
ApplyQuotas	bool
EnableMultiPOP	bool
MaxMessageCount	int
MaxDiskSpace	int
FwdAddress	string
FwdHost	string
FwdSendAs	string
FwdPort	string
NTAccount	string
MailFormat	string
AutoRespScript	string
AutoRespProcess	string
AddToList	string
RemoveFromList	string
PassMessageToProcess	bool
MaxUIDLCount	int
MaxMessageSize	int
RecurseIMAP	bool
MaxInactive	int
MaxMessageAge	int
MaxDeletedIMAPMessageAge	int
Comments	string
UserDefined	string

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

See:

Windows Account Integration 644

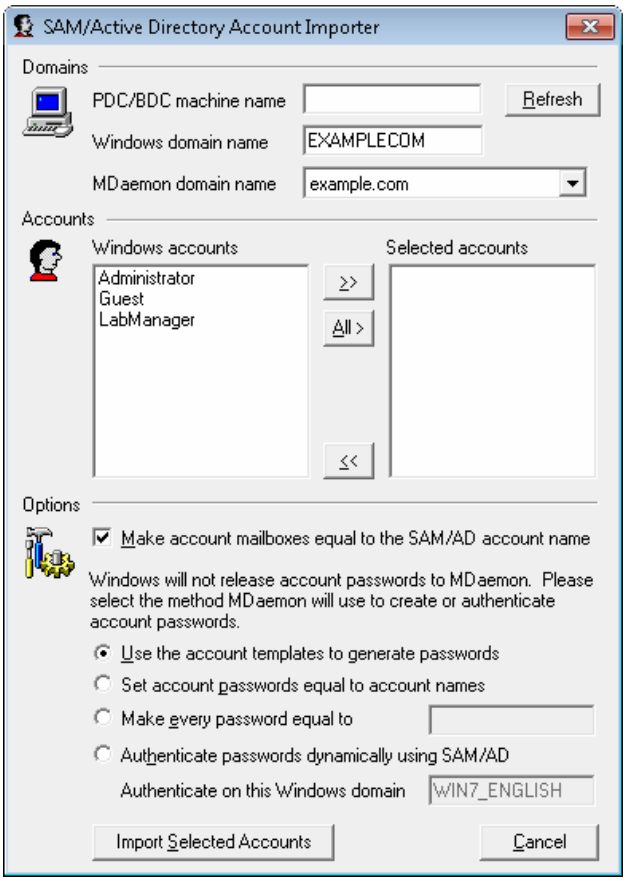
5.4.2 Windows Account Integration

MDaemon supports Windows Account integration. This support consists of a SAM/ Active Directory import engine, which can be reached from MDaemon's Accounts menu (Accounts » Importing... » Import accounts from SAM/Active directory...). Additionally, support for dynamic authentication of users is embedded into the MDaemon user management code. It is possible to specify a Windows domain in an account's password field and then MDaemon will dynamically authenticate such accounts in real-time, using the specified Windows domain's security system. Under such a scheme, changing the account's password in Windows user management will automatically update MDaemon. Therefore, your users will only have to remember one set of authentication credentials. This also makes for very easy account setup for new installations.

The security context of the account running MDaemon must have the **SE_TCB_NAME** privilege (i.e. "To act as part of the Operating System"). If the process is a service running in the *Local System* account, it will have this privilege by default. Otherwise, it must be set in the Windows user manager for the account under which MDaemon is running.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

SAM/Active Directory Account Importer



Domains

PDC/BDC Machine name

This field allows you to specify the machine name from which MDaemon will read Windows account database information. You can specify \\<DEFAULT> and MDaemon will read data from the local machine.

Refresh

Click this button to refresh the Windows Accounts listing.

Windows domain name

Type the Windows domain name from which you wish to import accounts.

MDaemon domain name

Choose from the drop-down list box the MDaemon domain into which the accounts will be imported.

Accounts

Windows accounts

This window contains a list of all the account names collected from the Windows account database.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Selected accounts
This window contains all the account names that you have selected and wish to import.

>>
Click this button to move the highlighted account names from the "Windows Accounts" window into the "Selected Accounts" window.

<<
Click this button to remove the highlighted entries from the "Selected Accounts" window.

Options

Make account mailboxes equal to the SAM/AD account name
Click this switch to force each imported user's Windows account name to be used as their Mailbox value. With this method, you will not need to worry about setting up the correct New Account Template 585 macros.

Use the account template to generate passwords
This option causes MDaemon to generate passwords for imported accounts using the account template settings (see Account Defaults 585).

Set account passwords equal to account names
This switch causes MDaemon to use the account name as the account password.

Make every password equal to...
This switch allows you to specify a static password value that will be used by all imported accounts.

Authenticate passwords dynamically using SAM/AD
This switch enables dynamic authentication of imported accounts. Rather than specifying a password MDaemon will simply authenticate the mail client supplied USER and PASS values using the NT database in real-time.

Authenticate on this Windows domain
Enter the name of the Windows domain that MDaemon will use when authenticating connections dynamically. **This is not the machine name of the domain controller. It is the actual name of the Windows Domain.**

When accounts are configured for dynamic authentication, the name of the Windows domain preceded by two backslash characters is used in the account's `PASSWORD` field and is stored unencrypted within the `USERLIST.DAT` file. For example, if an account is configured for dynamic authentication on a Windows domain called `ALTN`, the account's password field will contain the value `\\ALTN`. The two backslash characters preceding the domain name signify to MDaemon that the password field actually contains the name of a Windows

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

domain and that MDaemon should attempt to authenticate the USER and PASS values provided by the mail client using that domain's account database. For that reason you must not start a password with two backslash characters unless the account is configured for dynamic authentication as described above. In other words, you can't just have regular passwords that start with two backslashes. Passwords beginning with two backslashes are always assumed to be providing a Windows domain name and not a password.

You may enter the two backslashes and Windows domain name combination into an account's password field on the Account Details 521 screen of the Account Editor. You need not restrict yourself to using the importer in order to setup accounts for dynamic authentication.

See:

Importing Accounts From a Text File 642
Account Editor » Account 521

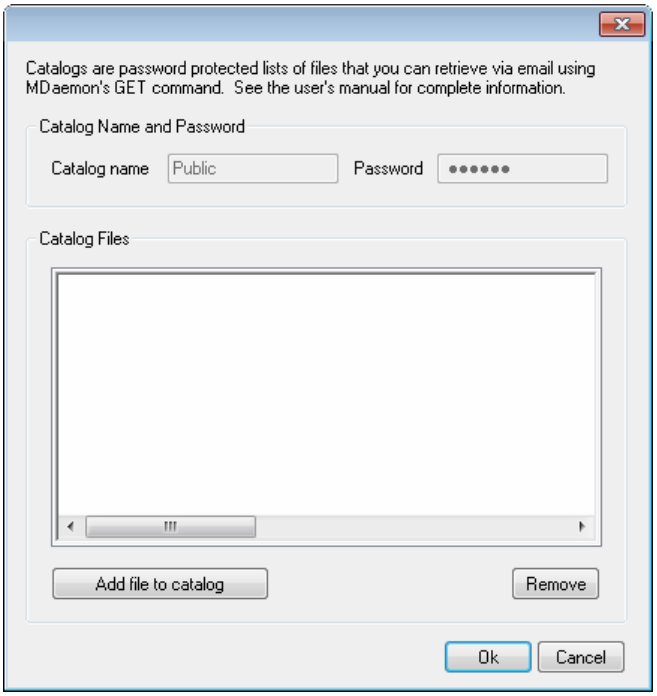
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Section VI

6 Catalogs Menu

6.1 Catalog Editor


Catalogs are password protected lists of files that you can retrieve via email using MDaemon's GET command. See the user's manual for complete information.
Catalog Name and Password
Catalog name
Public
Password
Catalog Files
Add file to catalog
Remove
Ok
Cancel

Use the Catalogs » New Catalog... or Catalogs » Edit Catalog... menu selection to open the Catalogs Editor for creating or editing a file catalog. Catalogs give users the ability to request files across the network and have them encoded and mailed back to them. Catalogs work by allowing the mail administrator to assign a "magic name" (i.e. shortcut) to files on disk. Magic names are like aliases which point to a specific file located somewhere accessible to MDaemon. A user can then use a special type of email message to request the file using the magic name. The format of this email message is described in the Remote Server Control 678 section (see the **GET** command in Mailing List and Catalog Control 678.

Catalog Name and Password

Catalog name
Use this field to enter a name for the file catalog.

Password
Use this field to enter a password for the file catalog.

Passwords are not required for all catalogs. You may choose to make catalogs accessible without a password.

See:

Mailing List and Catalog Control 678

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Catalog Files

This window displays all the files and their associated "magic names" currently registered as members of the specified catalog. Double click on an entry in this window to remove it from the catalog.

Remove
Click this button to remove a selected entry from the list of files.

Add file to catalog
Click this button if you wish to add a file to the catalog. After choosing the file that you wish to add, you will be prompted for the *Magic name* that you wish to assign to the file. Click Ok and the file and magic name will be added to the list.

The PUBLIC Catalog

The PUBLIC catalog is an exception to the normal rules governing access to file catalogs. Typically, to access a catalog requires a password that has been assigned to the catalog. With the PUBLIC catalog the password is not required. Files listed in the PUBLIC catalog are available to anyone who knows the file's magic name.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

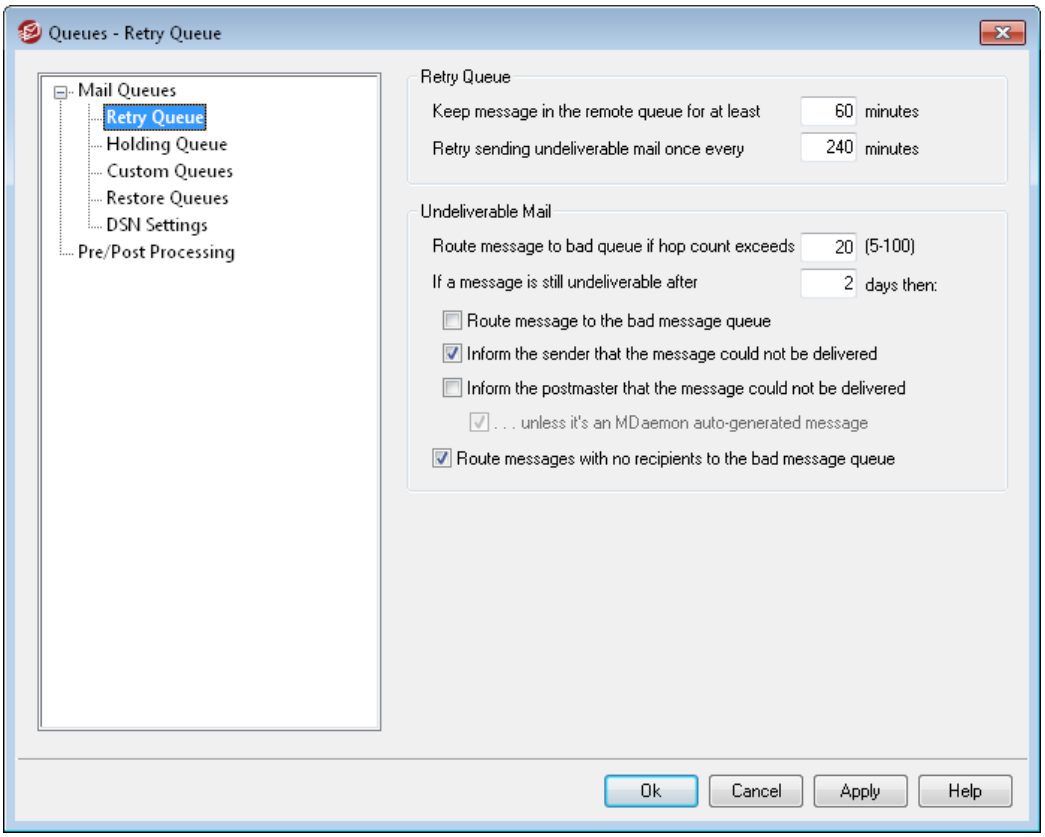
Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Section VII

7 Queues Menu

7.1 Mail Queues

7.1.1 Retry Queue



The Retry Queue dialog, located under Queues » Mail Queues, is used to determine how MDaemon will handle messages that cannot be delivered due to some non-fatal error, such as when the receiving server is temporarily unavailable.

Retry Queue

Keep message in the remote queue for at least XX minutes
This setting governs the length of time a message will remain in the remote queue before being removed and placed in the retry queue. The remote queue will generally attempt to deliver the message more frequently than the retry queue.

Retry sending undeliverable mail once every xx minutes
This setting determines how frequently the messages in the retry queue are processed.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Undeliverable Mail

Route message to bad queue if hop count exceeds (5-100)
RFC standards stipulate that a mail server must stamp each message each time that it is processed. These stamps can be counted and used as a stopgap measure against recursive mail loops that can sometimes be caused by errant configurations. If undetected, these looping message delivery cycles will consume your resources. By counting the number of times the message has been processed, such messages can be detected and placed in the bad message directory. The assumption is that if a message hasn't reached its recipient after being processed by a given number of mail servers then there is probably a mail loop in progress. Most likely, the default setting of this control should be sufficient to prevent mail loops and will not need to be changed.

If a message is still undeliverable after xx days then:
This setting determines the number of days that a message can remain in the retry queue before being removed. If you enter "0" days into this option then the message will be bounced back after the first retry attempt. The default setting is 2 days.

Route message to the bad message queue
When this option is enabled, a message will be moved to the bad message queue once it has reached the time limit set in the "*If a message is still undeliverable after xx days then:*" option.

Inform the sender that the message could not be delivered
Once a message has reached the time limit set in the "*If a message is still undeliverable after xx days then:*" option, this switch will cause MDaemon to send a message to the sender informing him that the message has been permanently removed from the server. The text of this message can be found (and edited) in the `DeliveryError.dat` file.

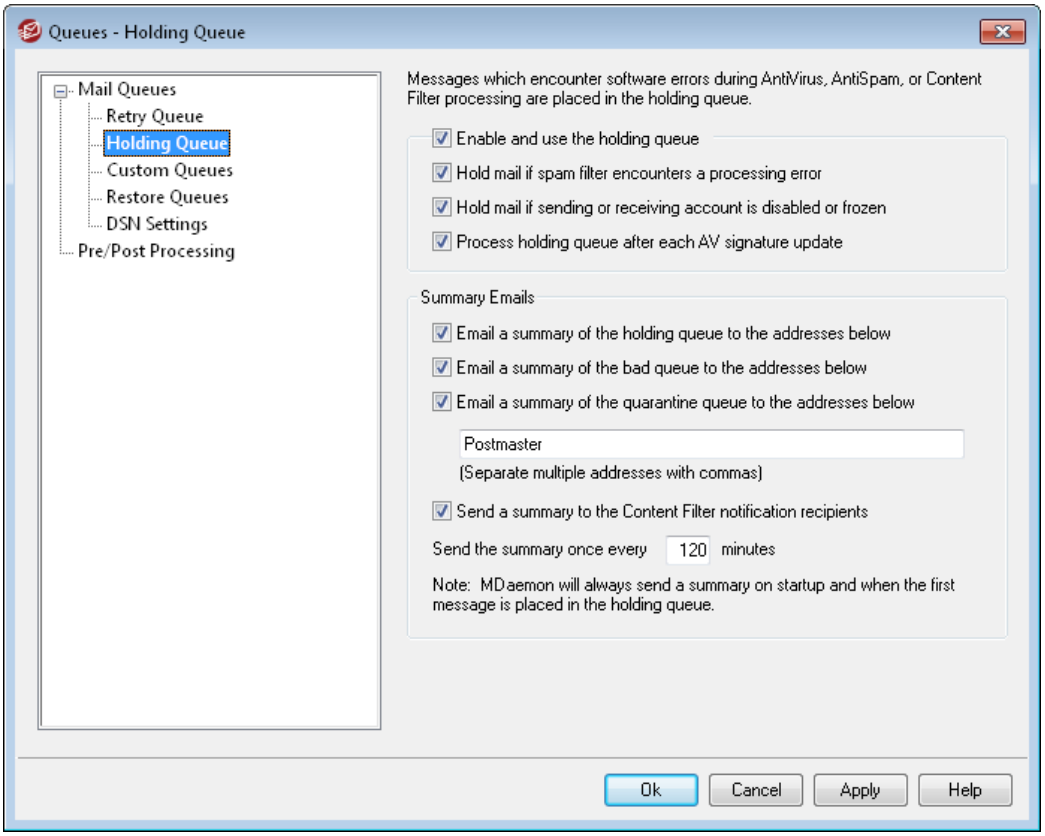
Inform the postmaster that the message could not be delivered
If this switch is enabled, the postmaster will be notified when a message has been permanently removed from the retry system.

. . . unless it's an MDaemon auto-generated message
By default, the retry system will not inform the postmaster that a message could not be delivered when that message was auto-generated by MDaemon. Clear this checkbox if you wish to inform the postmaster about the failure of those messages as well. Examples of auto-generated messages are return-receipt notifications, Autoresponder generated messages, results of account processing, and so on.

Route messages with no recipients to the bad message queue
When this option is enabled, messages with no recipient data will be moved to the bad message queue. When disabled, they will be deleted. This option is enabled by default.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

7.1.2 Holding Queue


Queues - Holding Queue
Mail Queues
Retry Queue
Holding Queue
Custom Queues
Restore Queues
DSN Settings
Pre/Post Processing
Messages which encounter software errors during AntiVirus, AntiSpam, or Content Filter processing are placed in the holding queue.
Enable and use the holding queue
Hold mail if spam filter encounters a processing error
Hold mail if sending or receiving account is disabled or frozen
Process holding queue after each AV signature update
Summary Emails
Email a summary of the holding queue to the addresses below
Email a summary of the bad queue to the addresses below
Email a summary of the quarantine queue to the addresses below
Postmaster
(Separate multiple addresses with commas)
Send a summary to the Content Filter notification recipients
Send the summary once every 120 minutes
Note: MDaemon will always send a summary on startup and when the first message is placed in the holding queue.
Ok
Cancel
Apply
Help

The Holding Queue, located under Queues » Mail Queues can be used to receive messages that cause software exceptions during AntiVirus, AntiSpam, or Content Filter processing. If a software error occurs when processing a message it will be moved into the holding queue and not delivered.

Messages placed into the holding queue will stay there until the administrator takes some action to remove them. There is a *Process Holding Queue* button on MDaemon's toolbar and an identical option on the Queues menu bar. You can also process the messages by right-clicking the holding queue on the main interface and then selecting "Re-Queue" from the right-click menu. Processing the holding queue will move all of its messages into either the remote or local queues for normal mail processing. If the error that caused a message to be placed into the holding queue still exists then that message will be placed back into the holding queue when the error reoccurs. If you want to attempt to deliver the holding queue's messages regardless of any error which might occur, then you can do so by right-clicking the holding queue on the main interface and then selecting "Release" from the right-click menu. When releasing messages from the holding queue a confirmation box will open to remind you that the messages could contain viruses or otherwise not be able to filter properly through the Content Filter, AntiSpam and/or AntiVirus engines.

Holding Queue

Enable and use the holding queue
Click this check box to activate the holding queue. Messages that cause software

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

exceptions during AntiVirus and Content Filter processing will be moved to this queue whenever an error occurs.

Hold mail if spam filter encounters a processing error
Click this option if you wish to move messages to the holding queue that cause errors during Spam Filter processing.

Hold mail if sending or receiving account is disabled or frozen
When this option is enabled, MDaemon will automatically hold messages when the sending or receiving account is disabled or frozen.

Process holding queue after each AV signature update
When this option is enabled, the holding queue will be processed automatically each time after the SecurityPlus for MDaemon 362 virus signatures are updated.

Summary Emails

Email a summary of the holding queue to the addresses below
If you wish to send a summary of messages contained in the holding queue to one or more email addresses at regular intervals then click this option and list the addresses in the text space provided below.

Email a summary of the bad queue to the addresses below
If you wish to send a summary of messages contained in the bad queue to one or more email addresses at regular intervals then click this option and list the addresses in the text space provided below.

Email a summary of the quarantine queue to the addresses below
Enable this option if you wish to send a summary of the quarantine queue at the designated interval below.

Summary message recipients
Use the text box to specify the email addresses to which you wish to send the queue content summaries designated in the previous two options. When listing multiple addresses, separate them with commas.

Notification messages are sent at MDaemon startup, the first time a message is placed into the holding queue, and at the interval specified in the *Send the summary once every XX minutes* option below.

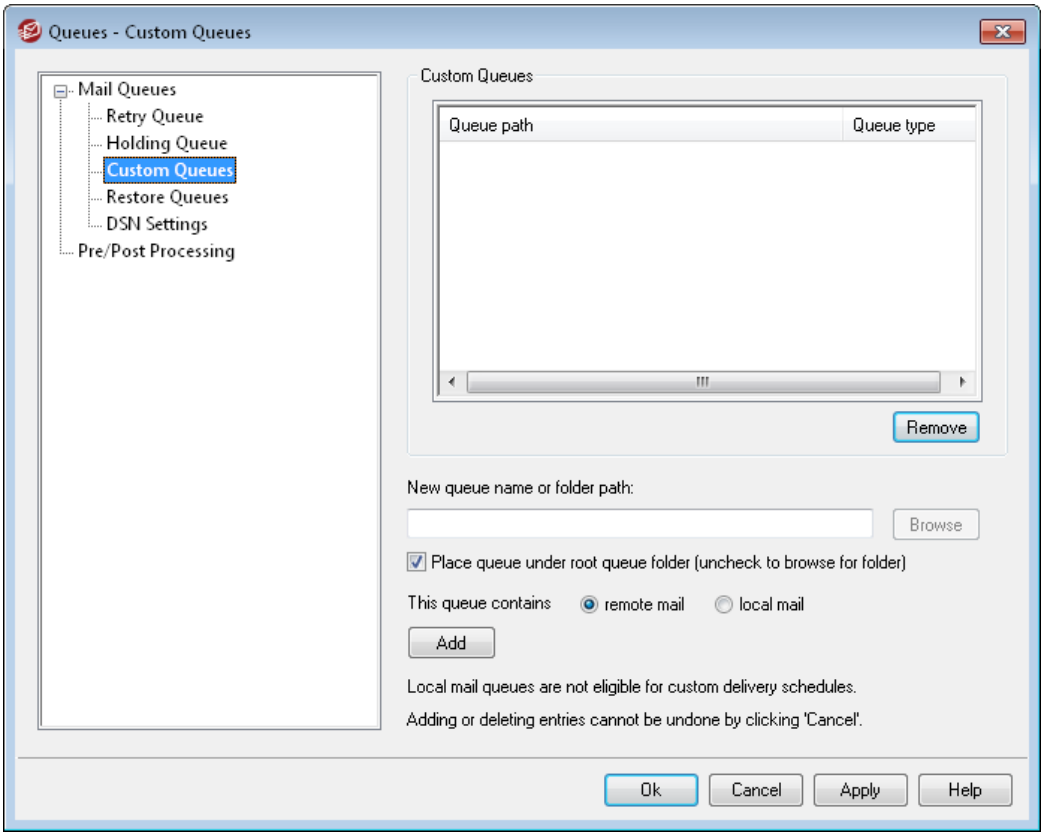
If a notification message causes a software error then it may not be delivered to remote recipients. It will, however, still be delivered to local recipients.

Send a summary to the Content Filter notification recipients
Click this option if you want an additional copy of each notification message to be sent to the Content Filter's designated notification Recipients 380.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Send the summary once every XX minutes
Use this option to designate the number of minutes that will pass before MDaemon will send a holding queue notification message to each specified address or Content Filter recipients.

7.1.3 Custom Queues



Use the Custom Queues dialog under Queues » Mail Queues to create custom local and remote mail queues. Custom queue support makes it possible for you to have MDaemon monitor several locations from which to send mail. You can create new queues and designate them as local or remote, and you can then use Content Filter rules to cause messages to be automatically placed into your custom mail queues, and for remote queues you can use the Event Scheduler 269 to create custom schedules to control how often those queues will be processed.

Custom Queues

This area displays an entry for each custom queue, listing its file path and whether it is local or remote.

Remove
If you wish to remove a queue from the list, select its entry and then click the *Remove* button.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

When you delete a custom queue, any custom schedules or content filter rules associated with that queue will also be deleted.

New queue name or folder path
Use this text field to specify the queue name or path to the folder that you wish to designate as a mail queue. If you wish to enter a full file path or browse to a specific folder, then clear the "*Place queue under root queue folder (uncheck to browse for folder)*" option below. If you do not clear that option then the queue will be created under MDaemon's `\queues\` folder.

Place queue under root queue folder (uncheck to browse for folder)
If this check box is enabled, the queue name specified in the "*New queue name or folder path*" option will be created as a subfolder under MDaemon's `\queues\` folder. If you disable this check box, the queue name specified will be created as a subfolder under MDaemon's `\app\` folder. When this option is disabled you can also type a full file path or use the Browse button to navigate manually to the folder you wish to use as a custom queue.

This queue contains...

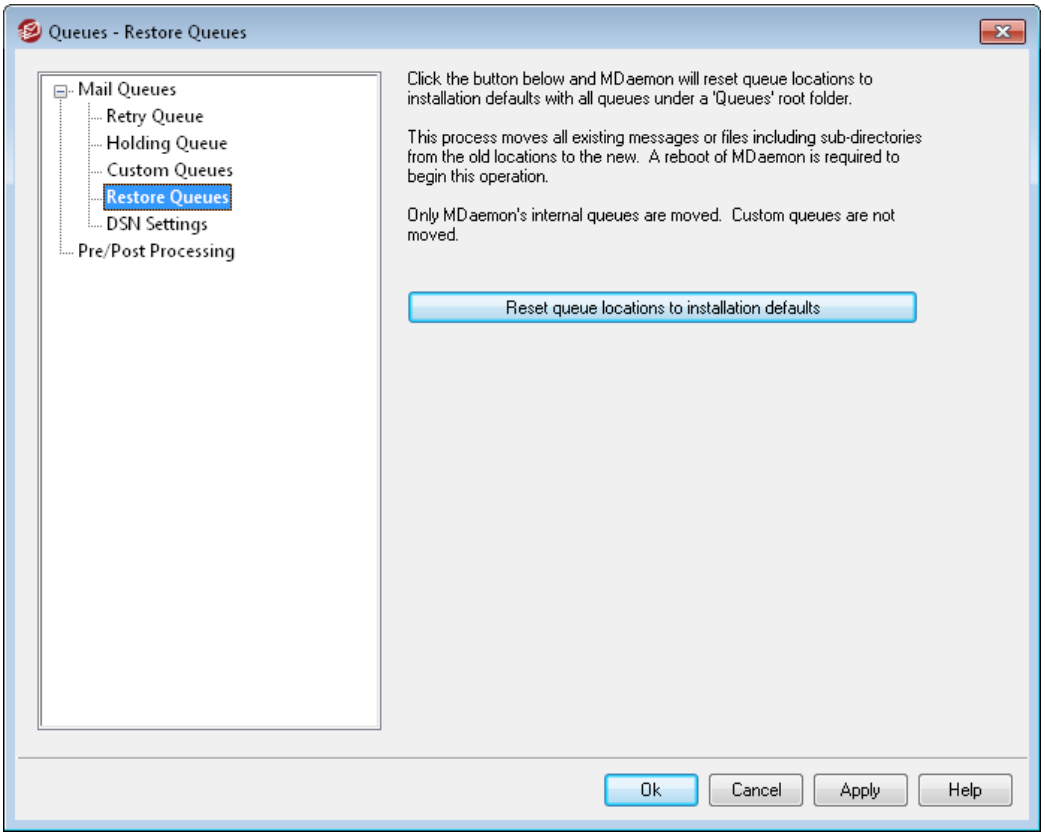
...remote mail
Choose this option if you want the custom mail queue to be used for remote mail.

...local mail
Choose this option if you want the custom mail queue to be used for local mail.

Add
After you have chosen the name, location, and type for your queue, click the *Add* button to add it to the list of custom queues.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

7.1.4 Restore Queues

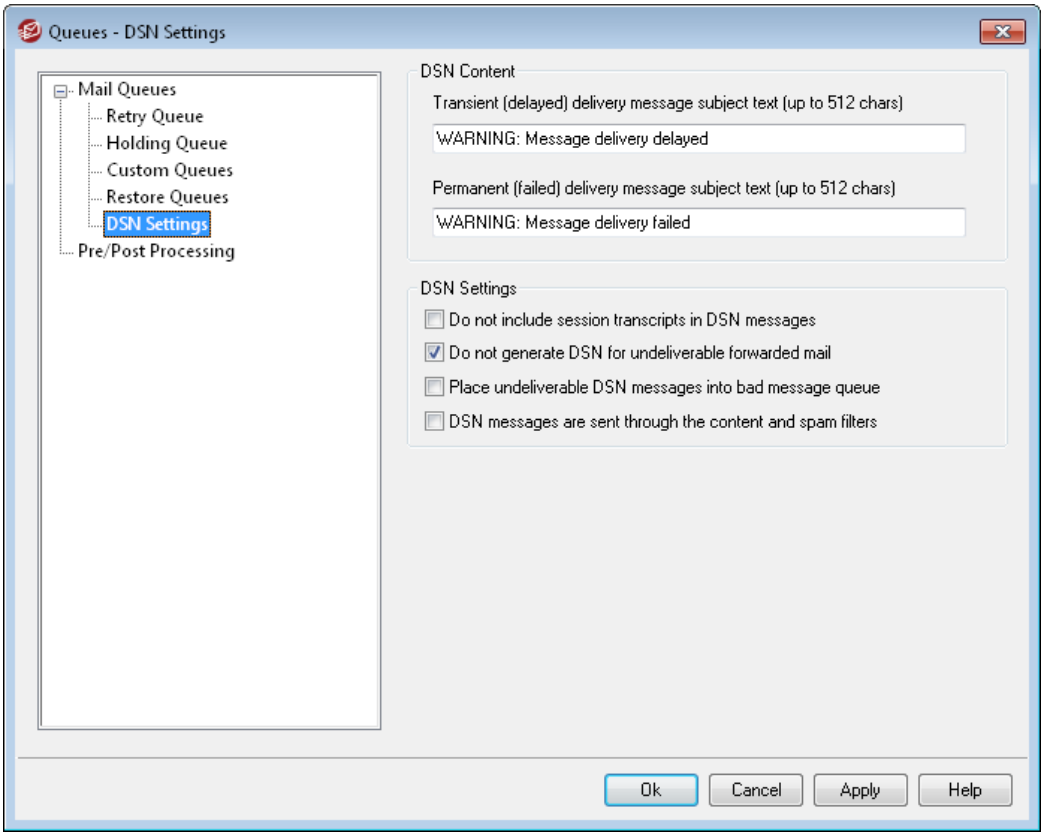

Queues - Restore Queues
Mail Queues
Retry Queue
Holding Queue
Custom Queues
Restore Queues
DSN Settings
Pre/Post Processing
Click the button below and MDaemon will reset queue locations to installation defaults with all queues under a 'Queues' root folder.
This process moves all existing messages or files including sub-directories from the old locations to the new. A reboot of MDaemon is required to begin this operation.
Only MDaemon's internal queues are moved. Custom queues are not moved.
Reset queue locations to installation defaults
Ok
Cancel
Apply
Help

Reset queue locations to installation defaults
By default, a new installation of MDaemon stores message queues such as Remote, Local, Raw, and the like under the `\MDaemon\Queues\` subfolder. Previous versions of MDaemon stored queues elsewhere. If your installation of MDaemon is using the old folder locations and you would like to move your queues to this more organized structure then click this button and all queues and the files and messages they contain will be moved for you. After clicking this button you will need to restart MDaemon for the changes to be implemented.

Custom Queues 658 will not be moved by this feature.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

7.1.5 DSN Settings


Queues - DSN Settings
Mail Queues
Retry Queue
Holding Queue
Custom Queues
Restore Queues
DSN Settings
Pre/Post Processing
DSN Content
Transient (delayed) delivery message subject text (up to 512 chars)
WARNING: Message delivery delayed
Permanent (failed) delivery message subject text (up to 512 chars)
WARNING: Message delivery failed
DSN Settings
Do not include session transcripts in DSN messages
Do not generate DSN for undeliverable forwarded mail
Place undeliverable DSN messages into bad message queue
DSN messages are sent through the content and spam filters
Ok
Cancel
Apply
Help

When MDaemon has a problem delivering a message, whether it is a temporary or permanent delivery failure, a Delivery Status Notification (DSN) message is sent to the sender of the message. This screen contains various options related to those DSN messages. It is located at: Queues » Mail Queues/DSN... » DSN Settings.

DSN Content

Transient (delayed) delivery message subject text (up to 512 chars)
This is the subject heading of the DSN message that will be sent when there is a transient problem causing a delay in message delivery. For example, if the recipient's mail server isn't available when MDaemon tries to deliver a message, MDaemon will continue trying to send it at designated intervals, and it will send this DSN message informing the sender of the problem. See: Customizing DSN Messages 662.

Permanent (failed) delivery message subject text (up to 512 chars)
This is the subject heading of the DSN message that will be sent when there is a problem that makes it impossible for MDaemon to deliver a message. For example, if the receiving mail server rejects the message, stating that the recipient's email address doesn't exist, MDaemon will stop trying to deliver the message and will send a DSN message informing the sender that the message cannot be delivered. See: Customizing DSN Messages 662.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

DSN Settings

Do not include session transcripts in DSN messages
Click this option if you do not wish to include SMTP session transcripts in delivery error and warning messages. This option is disabled by default.

Do not generate DSN for undeliverable forwarded mail
When this option is enabled, forwarded messages that encounter permanent, fatal delivery errors or expire from the Retry queue 654 will be moved to the bad messages queue, with no DSN messages being sent to the original sender. This option is enabled by default.

Place undeliverable DSN messages into bad message queue
Click this checkbox if you wish to place undeliverable Delivery Status Notification messages into the bad message queue rather than retrying them.

This only applies to DSN messages generated by MDaemon.

DSN messages are sent through the content and spam filters
Enable this option if you wish to send DSN messages through the content and spam filters. This option is disabled by default.

Customizing DSN Messages

The "human-readable" portion of transient (delayed) and permanent (failed) DSN messages can be customized by creating a file called `DSNDelay.dat` or `DSNFail.dat` respectively, in the `\MDaemon\App\` folder. Edit them with a text file editor such as Notepad and enter the text you wish to use. The following macros can be used in your custom text:

$SESSIONID$ - expands to the delivery session's ID string

$QUEUEID$ - expands to the message's mail queue ID string

$MESSAGEID$ - expands to the message-id header value

$RETRYDAYS$ - length of time allowed in queue (in days)

$RETRYHOURS$ - length of time allowed in queue (in hours)

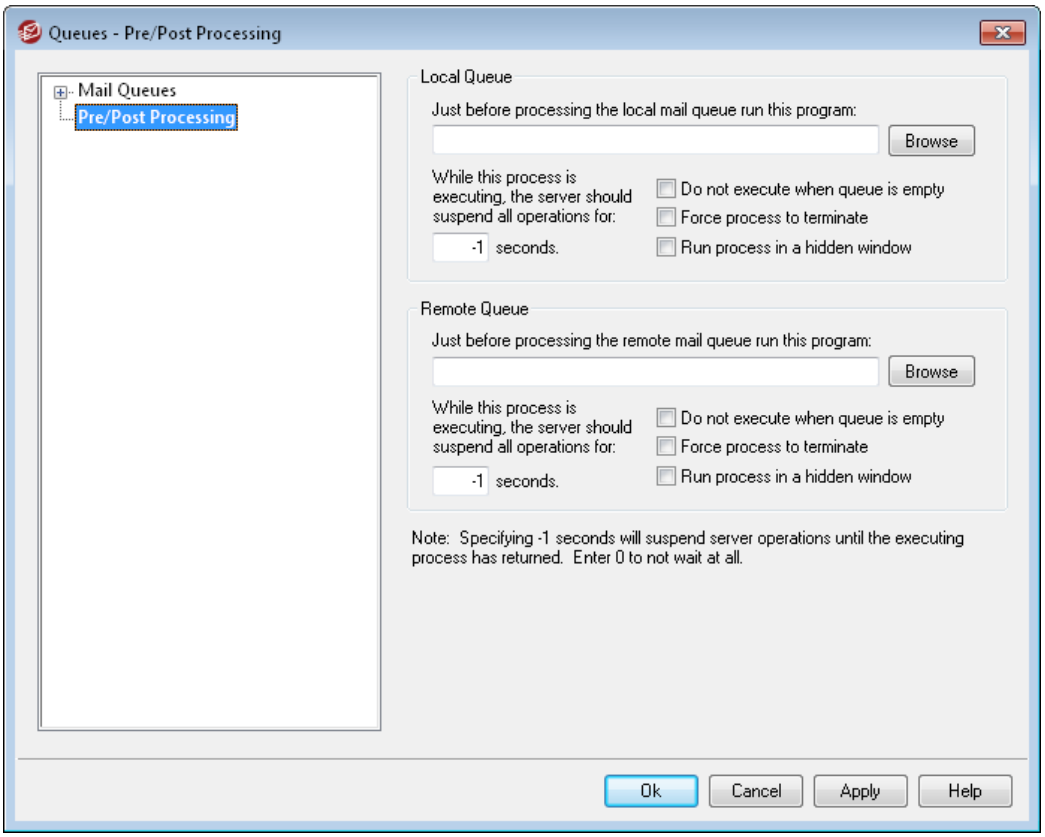
MDaemon must be restarted before changes to these files are loaded.

See:

Retry Queue 654

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

7.2 Pre/Post Processing


Queues - Pre/Post Processing
Mail Queues
Pre/Post Processing
Local Queue
Just before processing the local mail queue run this program:
Browse
While this process is executing, the server should suspend all operations for:
-1 seconds.
Do not execute when queue is empty
Force process to terminate
Run process in a hidden window
Remote Queue
Just before processing the remote mail queue run this program:
Browse
While this process is executing, the server should suspend all operations for:
-1 seconds.
Do not execute when queue is empty
Force process to terminate
Run process in a hidden window
Note: Specifying -1 seconds will suspend server operations until the executing process has returned. Enter 0 to not wait at all.
Ok
Cancel
Apply
Help

Local and Remote Queue Pre/Post Processing

Just before processing the (local/remote) mail queue run this program
This field specifies a program path and name that will be executed just prior to the processing and delivery of any RFC-2822 messages that might be in the local or remote message queues. If complete path information is not provided, MDaemon will first search for the executable in the MDaemon directory, then in the Windows System directory, next in the Windows directory, and finally the directories listed in the PATH environment variable.

...suspend all operations for xx seconds
The value entered here determines how MDaemon will behave while the specified program is in progress. MDaemon can be configured to pause its execution thread for the number of seconds specified while waiting for the process thread to return. If the process returns before the number of seconds has elapsed, MDaemon will resume its execution thread immediately. If you enter "0" in this option MDaemon will not suspend operations at all. Entering "-1" will cause MDaemon to wait until the process returns, no matter how long that might be.

Do not execute when queue is empty
Enable this switch if you do not want the specified program to run when the queue is empty.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Force process to terminate
Sometimes the process you need to run may not terminate on its own. This switch will cause MDaemon to force the session to terminate once the time specified in ...*Suspend all operations for XX seconds* has elapsed. This switch does not work if the elapsed time interval is set to "-1".

Run process in a hidden window
Click this checkbox if you want the process to run in a hidden window.

7.3 Queue and Statistics Manager

MDaemon's Queue and Statistics Manager is accessed from within MDaemon under the Queues » Queue and Statistics Manager menu selection. The Queue and Statistics Manager is made up of a four-page dialog. Each of these pages has been designed to serve a distinct and specific purpose while also maintaining a simple format that makes them very easy to use.

Queue Page 665

The default tab is the *Queue Page*. From this page you can easily manage all of MDaemon's standard mail queues, as well as the User Account mailbox folders. By simply clicking on the queue or user of your choice, a list of all message files contained within the specified queue will be displayed along with several key pieces of pertinent information about each message: the sender, the recipient, the content of the "Deliver-To" header, the subject of the message, its size, and how long it has been at its current location. In addition, controls are provided that make it easy to copy or move messages between folders, or delete them completely.

User Page 668

The *User Page* displays a list of all MDaemon users. This list includes their full name, mailbox name, the number of messages in their mailbox, the amount of disk space that their account is taking up, and the date that they last checked their mail. This list can also be saved to disk as a text file, or it can be saved in comma delimited format for use with databases.

Log Page 670

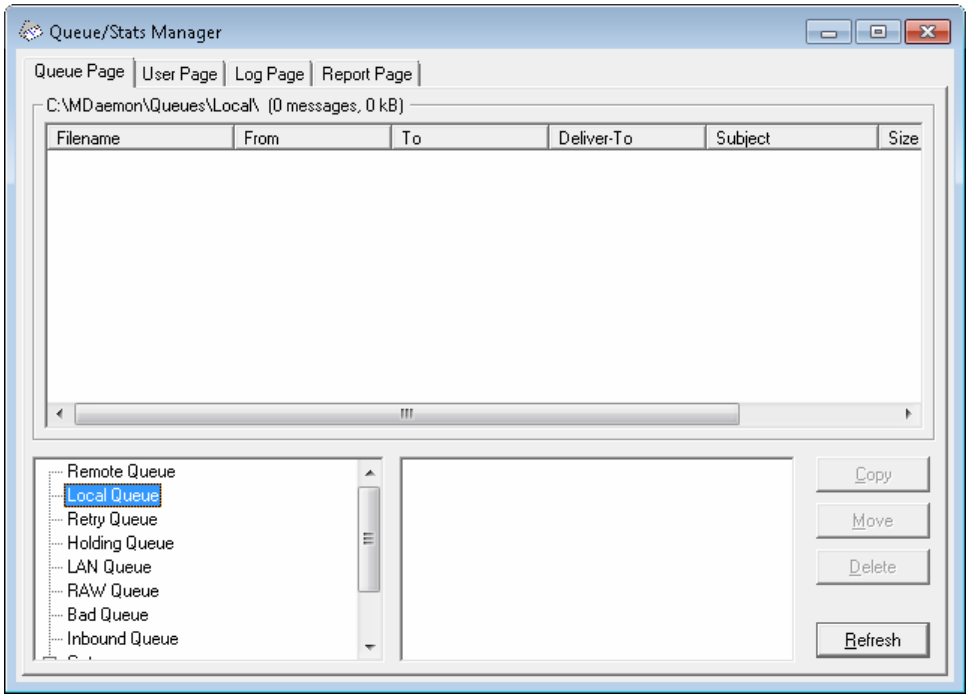
With this dialog you can display MDaemon's *Log Files* in a simple list format. This feature is very useful for quickly examining the history of MDaemon's mail transactions because it condenses the selected *Log File* into a columnar list which contains: the Type of the message (POP Inbound, DomainPOP, RFC2822, and so on), the Host to which MDaemon connected during the transaction, the sender, the recipient, the message size, the date that each message was processed, and whether or not the transaction was successful. You can also examine the detailed portion of the log regarding any of the entries on the list by double clicking the desired entry. This will display the portion of the log where that transaction was made. Logs displayed on the *Log Page* can be saved as a text file or in comma delimited format for use with databases.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Report Page

The last tab is the *Report Page*. With this feature you can produce a report containing all of MDaemon's configuration settings, written in a plain text readable format. Because of the large number of optional settings and configurations in MDaemon, this can greatly speed the process of administering configuration changes as well as aid in diagnosing possible configuration problems. Additionally, this report is displayed in a text editable format that makes it possible to Copy/Paste the information it contains (using the right-click shortcut menu), or add notations or other information to the file before saving it.

7.3.1 Queue Page



Queue page list box

When a queue or user is chosen from the *Message Queues* area or the user list box beside it, a list of all message files contained within the selected queue will be displayed in the main list box on this page. This list contains each message's file name, the sender, the recipient, the content of the "Deliver-To" header, the subject of the message, its size, and how long it has been at its current location (listed by date and time).

Above this box the complete file path to the currently displayed directory is given, as well as the number of messages displayed and the size of the directory.

You may copy, move, or delete one or more files by selecting them from the list and then clicking the appropriate button below it.

The content of these files may also be edited directly from the *Queue Page* list box.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Simply double-click the file that you wish to edit (or choose "Edit" from the right-click shortcut menu) and the file will be opened in Notepad for editing.

If you want the Queue and Statistics Manager to open an editor other than Notepad by default, then you must edit the `mdstats.ini` file located in the `\MDaemon\app\` folder. Change the "`Editor=`" key located under the `[QueueOptions]` section heading to `Editor=MyEditor.exe`. If the file path of the `*.exe` file is not in your current path, then you will have to include the path here as part of the file name.

The list box can be navigated by using the vertical or horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can sort information contained in the *Queue Page* list box by whichever column you choose. Simply click once on the desired column to sort it in ascending order (A-Z, 1-2), or click twice to sort it in descending order (Z-A, 2-1). Columns can also be resized by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width.

Selecting Files

To select files individually	Click the desired file.
To select contiguous files	Click the first file in the contiguous list of files that you wish to select, then while holding down the SHIFT key, click the last contiguous file in the desired list. Alternatively, you may use the ARROW, HOME, END, PAGE UP, and PAGE DOWN keys, while holding down the SHIFT key, to select files in contiguous order.
To select non-contiguous files	Click on the desired files in the **File Name** column while holding down the CTRL key.

Message queues
Click an in the lower left pane and a list of all files contained within the specified queue will be displayed in the *Queue Page* list box. If you click the *User Folders* option, a list of all MDaemon users will be displayed in the *User List Box* to the right of the *Message Queues* section.

Users list box
This box displays a list of all MDaemon users when the *User Folders* option is clicked in the *Message Queues* section (lower left pane). Click a user's name to display a list of all message files currently contained in the user's mailbox folder.

Refresh
Because mail queues are dynamic while MDaemon is active - with message files constantly being transferred to and from them - you should regularly click this button to refresh any list of files that you may have displayed.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

You can edit the MDstats.ini file to cause displayed lists to automatically refresh. To do this simply open the MDstats.ini file located in MDaemon's \app\ directory and edit the AutoRefresh key under the [QueueOptions] heading to reflect the number of seconds that you wish to elapse between refreshes. Entering the value "0" means that you do not want the list to automatically refresh. Example: AutoRefresh=15 (the list would refresh every 15 seconds).

Copy
When one or more files are selected, click this button to copy the selected files to another queue or user's mailbox folder. After clicking this button the *Copy Message(s)* dialog box will open, from which you can select the desired location to which you wish to copy the selected files.

Move
When one or more files are selected, click this button to move the selected files to another queue or user's mailbox folder. After clicking this button the *Move Message(s)* dialog box will open, from which you can select the desired location to which you wish to move the selected files.

Files copied or moved to other queues will rarely retain their original file names. To avoid overwriting files of the same name that may already be in the queue, MDaemon always calculates the next destination filename based on the HIWATER.MRK file located in the destination folder.

Delete
When one or more files are selected in the *Queue Status List Box*, click this button to delete the selected files. After clicking this button a confirmation box will open asking if you really do wish to delete the selected files.

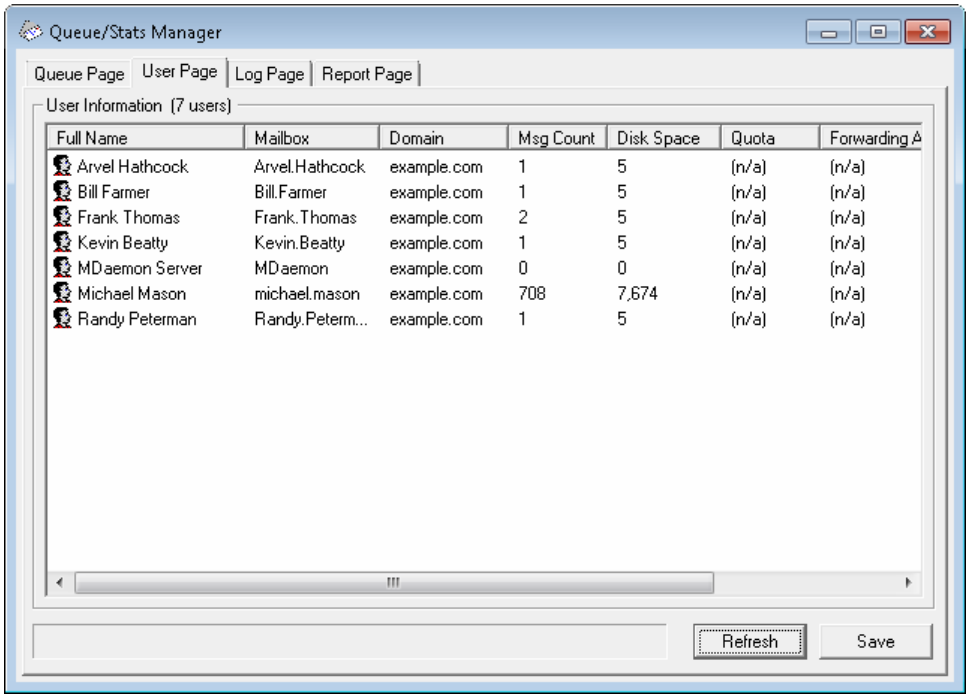
Mail queues are dynamic while MDaemon is active - with message files constantly being transferred to and from them. For this reason you should be aware that when copying, moving, or deleting files you may at times encounter a message stating that the action that you are attempting cannot be completed. This will occur when the message file that you are attempting to work with has already been removed by MDaemon before the desired action has begun. By clicking the *Refresh* button, you can update the current list of files displayed in the list box.

You can prevent messages from being moved out of the queue while you are editing them by editing the MDstats.ini file. To do this simply open the MDstats.ini file located in MDaemon's \app\ directory and change the LockOnEdit=No key under

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

> the `[QueueOptions]` heading to `LockOnEdit=Yes`. This will cause a `LCK` file to be created whenever you are editing a message, which will prevent it from being moved out of the queue until you are finished with it.

7.3.2 User Page



User information
When the *User Page* is chosen, a list of all MDaemon accounts is loaded into the *User Information* list box. This list contains each user's full name, the name of their mailbox, the domain to which the account belongs, the number of messages it contains, its mail format, the amount of disk space (in kilobytes) that the account is taking up, their forwarding address, and finally, the date that their mail was last checked. Given that the information contained in this list is constantly changing, it can be easily updated by clicking the *Refresh* button.

The list box can be navigated by using the vertical and horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can sort information contained in the *User Information* list box by whichever column you choose. Simply click once on the desired column to sort it in ascending order (A-Z), or click twice to sort it in descending order (Z-A). Columns may also be resized by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width. Further, you can double-click any entry and MDStats will be shifted to the *Queue Page* with the contents of their mailbox folder displayed.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

By default, the list displays the Message Count not file count, and the Disk Space used *by messages* not the space used by all files in the directory. This is the *Quota* information reported by MDaemon. Alternatively, you can display the *file* count and disk space used by all *files* instead of by messages. To change this setting simply open the `MDstats.ini` file located in MDaemon's `\app\` directory and change the `ShowQuota=Yes` key under the `[UserOptions]` heading to `ShowQuota=No`.

User folders contain a file called "`hiwater.mrk`" which is used to determine some of this user information. You should avoid deleting this file unnecessarily as it will prevent the Queue and Statistics Manager from being able to obtain some of the information listed in the *User Information* list box.

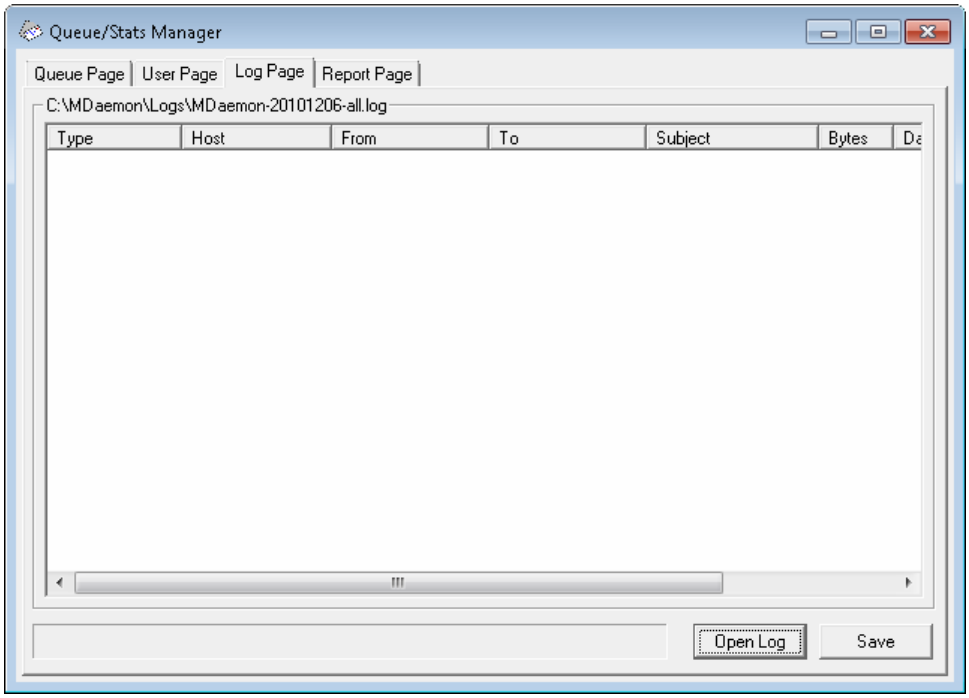
Refresh
User statistics such as the number of messages contained in their mailboxes, and the amount of disk space that their accounts are using, are constantly changing. You can easily update the information contained in the *User Information* list box by clicking the *Refresh* button. This will immediately make all displayed information current.

Progress indicator
Because *User Information* lists can at times be very large, below the *User Information* list box is a progress indicator bar that provides a visible indication that the program is still operating when large files are being loaded.

Save
The information contained in the *User Information* list box can be saved as a file in comma delimited format for use with databases, or as a plain ASCII text file by clicking the *Save* button. After choosing a name and location for this file in the Windows Save As dialog, you will be asked whether you want to save the file in comma delimited format or as a plain text file.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

7.3.3 Log Page



Log report
The *Log Report* list box displays MDaemon's detailed log files that you select through the *Open Log* button and the Windows Open dialog that follows it. The *Log Report* display provides a quick and easy way to review the history of mail transactions that MDaemon has processed without having to sort through the large volume of information that MDaemon log files may sometimes contain. When a *Log Report* is displayed in this list box the Queue and Statistics Manager breaks it down into a simple format containing: the Type of the message (POP Inbound, DomainPOP, RFC2822, and so on), the Host to which MDaemon connected during the transaction, the sender, the recipient, the message size, the date that each message was processed, and whether or not the transaction was successful.

You can also examine the detailed portion of the log regarding any of the entries on the list by double clicking the desired entry. This will display the portion of the log where that transaction was made. Using the right-click shortcut menu you can copy/paste this detailed log portion to a text editor for saving or editing should you desire to do so.

The list box can be navigated by using the vertical and horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can resize the list box's columns by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width.

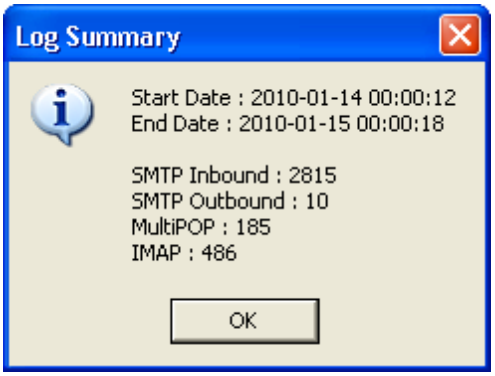
The *Log Page* will display log files that have been compiled using either the *Log detailed mail sessions* or the *Log summarized*

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

> *mail sessions* option located under Logging » Log Mode. However, we highly recommend that you use the *Log detailed mail sessions* option. When using the *Log summarized mail sessions* format you will find that there is very little information that will be displayed in your *Log Report*. Because the *Log Page* itself condenses the detailed log into a summary view of MDaemon's activity, while still providing the ability to look at the detailed view of every transaction when necessary (by double-clicking an entry), there is no need to have MDaemon summarize the log file while compiling it.

Open log
Click this button to open the Windows Open dialog for choosing which log file that you wish to view. If you click this button when there is a *Log File* already displayed in the *Log Report* list box, you will be given the option to append the new file to the one that is already displayed.

After a log is displayed, a message box will be opened which contains a summary of the selected log. When saving a Log Report as a text file, this log summary will be appended to it.

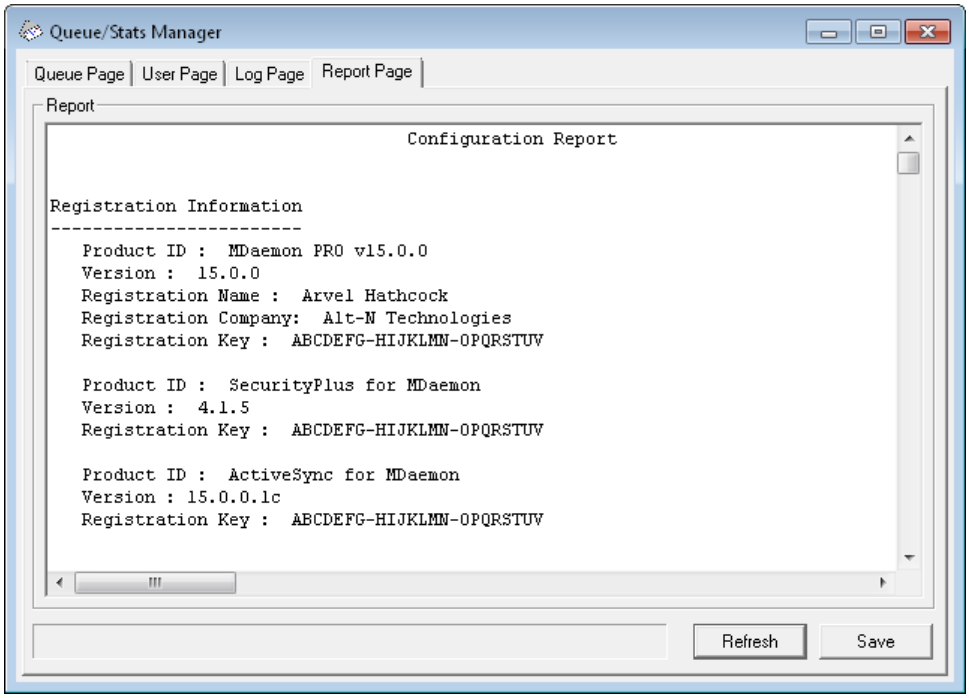


Progress indicator
Because *Log Files* can be very large, below the *Log Report* list box is a progress indicator bar that provides a visible indication that the program is still operating when large files are being loaded or saved.

Save
The information contained in the *Log Report* list box can be saved as a file in comma delimited format for use with databases, or as a plain ASCII text file by clicking the *Save* button. After choosing a name and location for this file in the Windows Save As dialog, you will be asked whether you want to save the file in comma delimited format or as a plain text file.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

7.3.4 Report Page



Report
When the *Report Page* is clicked, a comprehensive report will be produced that lists every setting within MDaemon in an easily readable text format. This feature greatly decreases the amount of time needed by an administrator to check MDaemon's many configuration settings, and it can aid in quickly solving possible configuration problems.

You can navigate through this report using either the scroll bars or the CURSOR keys, and the *Report* display is also a text editor - making it possible to insert notations or additional information that you may want on the report before saving it to a file. Additionally, you can use the shortcut menu to Cut, Copy, and Paste, to and from this display by right-clicking your mouse and making the desired selection from the menu that opens.

Refresh
Click this button to update the currently displayed *Report* of MDaemon settings.

Progress indicator
As with the other tabs in the Queue and Statistics Manager, the *Report Page* contains a progress indicator bar that serves as a visible indicator that the program is still operating while large files are being loaded or saved.

Save
Click this button to save the currently displayed *Report*. After clicking this button a standard Save As dialog will open so that you can designate a file name and location where you want to save it.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

7.3.5 Customizing the Queue and Statistic Manager

7.3.5.1 MDstats.ini File

Customizing the Queue/Statistic Manager

The following is a list of settings that can be modified in the `MDstats.ini` file located in MDaemon's `\app\` directory:

[MDaemon]

AppDir=C:\mdaemon \app\	Location of MDaemon's \app\ directory.

[QueueOptions]

Editor=NOTEPAD.EXE	Editor to use when a message is double-clicked, or when a message is right-clicked and then Edit is selected.
LockOnEdit=No	Whether or not to create a LCK file when editing a message. This will prevent a message from being moved out of the queue while it is being edited.
AutoRefresh=Yes	Time (in seconds) between auto refreshes of the message listing. 0 means no auto refresh.
ShowDirectories=Yes	Show subdirectories of the queues in the list box in addition to the messages. Directories will appear as <DirectoryName>.

[UserOptions]

ShowQuota=Yes	Determines whether the user listing displays quota information (message count and disk space just like MDaemon calculates it) or file information (number of files and total disk space).

[LogOptions]

ShowUnknown=Yes	Show sessions that MDStats couldn't determine if they were inbound or outbound, SMTP or POP.
ShowSmtpInbound=Yes	Show SMTP inbound sessions.
ShowPopInbound=Yes	Show POP inbound sessions (mail checks).
ShowSmtpOutbound=Yes	Show SMTP outbound sessions.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

ShowPopOutbound=Yes	Show POP outbound sessions (MultiPOP, DomainPOP).
ShowRFC822=Yes	Show RFC822 local mail deliveries.
ShowSmtpHelo=Yes	For SMTP inbound sessions, show HELO domain in the Host column.
IgnoreEmptyPop=Yes	Ignore mail checks when no mail was deliverd.
ShowImap=Yes	Shows IMAP Sessions.
[Remap]	Drive letter remapping; for running MDStats from a different machine than the one MDaemon is on.
C:=\\server\c	When reading from MDaemon.ini, replace "C:" with "\\server\c".
[Special]	
OnlyOneInstance=No	Allow only one instance of MDStats to run. Attempting to open it again will activate the instance that is already running.

See:

MDStats Command Line Parameters 674

7.3.5.2 MDStats Command Line Parameters

Note: All command line parameters are not case sensitive.

Number 1 through 8	Display a specified queue in the Queue Page. = Remote Queue = Local Queue = Retry Queue = LAN Queue = RAW Queue = Bad Queue = SmtpIn Queue = Save Queue

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

/L[N] [InputFile] [OutputFile]	Produce a log file report. Specifying an "N" after the "L" means do not save as a comma delimited file.
/A	If producing a log file report, append new information to the output file rather than overwriting it.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Section VII

8 Additional MDaemon Features

8.1 MDaemon and Text Files

MDaemon uses a number of plain text files to store some of its data, system generated message templates, and configuration settings, which provides a great deal of flexibility. You can create new text files from within MDaemon by using the File » New menu selection. This can be useful for quickly creating data files for use with Autoresponders and various other MDaemon features, such as RAW files.

Editing MDaemon Files

MDaemon's various data files are plain text and can be edited in Notepad. You can easily open any of these files from within MDaemon by using the File » Open » Empty Text File menu selection. By default this looks in MDaemon's `\app\` folder for `*.txt` files. Switch the *Files of type:* drop down list to "All files" to see the rest of the files contained in that folder.

8.2 Remote Server Control via Email

Many functions of MDaemon can be accessed remotely using the email transport system itself, by sending a specially formatted email to the MDaemon system account, "`MDaemon@<MDaemon's Domain>`". Messages sent to the server are stored in the server's message directory just like any other user.

Some of these control messages require a valid account on the server. For those commands which require a valid account, the message must be authenticated during the SMTP process using SMTP AUTH.

There are two, broad categories of commands that can be used in email messages: Mailing List and Catalog 678, and General Email 681.

See:

Mailing List and Catalog Control 678
General Email Controls 681

8.2.1 Mailing List and Catalog Control

None of these commands require an account on the server. Parameters contained in [brackets] are optional. For example: "name [address]" could be entered as "Michael" alone or with the optional parameter added: "Michael user1@example.com". Messages should be sent to "mdaemon@[MDaemon domain]" with the each command and associated parameters contained on a single line in the body of the message.

COMMANDS	PARMS	DESCRIPTIONS

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

SUBSCRIBE	listname [address] [{real name}] [(pass)]	The originator is added to the membership of the specified list provided that list exists and allows remote subscriptions. If an optional address is specified after the list name then that address is added to the list's membership rather than the address found in the FROM: field of the subscription message. A real name can be added for the subscriber by including it in braces (e.g. {Bill F}. If the list's password follows this command (parentheses around it are required) then the command will be honored even if this list's subscribe function is switched off.
		Examples:
		`SUBSCRIBE mdsupp`
		`SUBSCRIBE mdsupp me@example.com {Bill F}`
		`SUBSCRIBE mdsupp you@example.org (PASS)`

UNSUBSCRIBE
Or
SIGNOFF
	listname [address] [(pass)]	The originator is removed from the membership of the specified list provided that list exists and contains the originator as a current member. If an optional address is specified after the list's name then that address is removed from the list's membership rather than the address found in the FROM: field of the unsubscribe message. If the list's password follows this command (parentheses around it are required) then the command will be honored even if this list's unsubscribe function is switched off.
		Examples:
		`UNSUBSCRIBE MDSUPP (MDSPASS)`
		`SIGNOFF MDSupportList me@example.com`

DIGEST	listname [address]	The sender is set to receive mail from the list in digest format. If an optional address is specified after the list name then that address is set to digest mode.
		Examples:
		`SET DIGEST MDSupportList`
		`SET DIGEST mdsupp user1@example.com`

NORMAL	listname [address]	The sender is set to receive mail from "list" in normal (non-digest) format. If

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

		an optional address is specified after the list name then that address is set to receive in normal format instead of the sender.
		Examples:
		`NORMAL MDSupportList@example.com`
		`NORMAL mdsupp@example.com user1@altn.com`

NOMAIL	listname [address]	This command sets 'address' to nomail mode. The account will enter a suspended state and will no longer receive list traffic. If no address is specified then the originator of the message will be used. Example: `NOMAIL list@example.com me@example.com`

MAIL	listname [address]	This command returns 'address' to normal mode from nomail mode. If no address is specified then the originator of the message will be used.
		Examples:
		`MAIL list@example.com`
		`MAIL list@example.com me@example.com`

REALNAME	listname [address] {real name}	This command sets the real name value for "address" who is a member of list "listname" to the given value. The real name must be enclosed in { and } characters. Example: `REALNAME mdsupp@altn.com {Bill Farmer}`
GET	catalog magic-name (password)	Retrieves a file from the specified catalog, MIME encodes it in an email message, and sends that message to the originating account or to the one specified in a RESULTS TO directive. Example: `GET utils myutil (mypass)` **NOTE**: The special PUBLIC catalog doesn't require a catalog name or password in order to retrieve a file.
DIR	catalog	Retrieves a directory of the files and magic names available through the catalog.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

		Example: `DIR public`
`LIST`	[listname] [list password]	Provide information about a mailing list. If the list's name is not provided, then a summary of all lists is returned. If the lists password is provided then a greater level of information about the list is returned. Example: `LIST MyList@example.com Lz$12`

See:

Remote Server Control Via Email 678
General Email Controls 681

8.2.2 General Email Controls

These are general email commands that can be sent to the system account via email messages. Messages should be sent to "mdaemon@[MDaemon domain]" with the each command and associated parameters contained on a single line in the body of the message.

COMMANDS	PARMS	DESCRIPTIONS
`HELP`	none	A copy of the NEWUSERHELP.DAT is processed and mailed back to the message originator.
`STATUS`	none	A status report on server operations and current conditions will be mailed back to the message originator. Since the information contained in this status report is considered private, the user requesting the report must be authenticated as an administrator. Example: `STATUS`

See:

Remote Server Control Via Email 678
Mailing List and Catalog Control 678

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

8.3 The RAW Message Specification

8.3.1 The RAW Message Specification

MDaemon has inherent support for a simple and powerful mail message format known as RAW mail. The purpose of the RAW mail system is to provide a simple and standard format that software systems such as MDaemon can use to create much more complex RFC-2822 compliant message. Use of mail transport agents such as RAW allow client software to offload to the server all the complicated work of maintaining adherence to Internet mail standards.

RAW mail consists of a series of required and optional text headers followed by a message body. Most headers consist of a token followed by a value enclosed in <> symbols. Each header line ends with a <CRLF> combination of characters. Headers are separated from the message body by a blank line and are case insensitive, and the *from* and *to* headers are the only ones that are required. All text, headers and body, are plain ASCII text and must be contained in a file that ends with the extension, "`.raw`" (for example "`my-message.raw`"). Then, to queue the message for delivery, place the `*.raw` file in MDaemon's RAW queue (typically located at, "`C:\MDaemon\Queues\Raw`").

Bypassing the Content Filter

By default, RAW messages are passed through the Content Filter like normal messages. If you want a given RAW message to bypass the filter then start the name of the file with "`p`" or "`P`". For example, "`P_my-message.raw`" would bypass the Content Filter but "`my-message.raw`" would be processed through it normally.

Bypassing the Content Filter will prevent messages from being DKIM signed. If you have configured MDaemon to sign all messages then this could potentially cause some delivery problems. If you want MDaemon to sign RAW messages configured to bypass the Content Filter then you can do so by using the `x-flag=sign` option outlined below.

RAW Headers

From <mailbox@example.com>	This field contains the email address of the sender.
To <mailbox@example.com [, mailbox@example.com]>	This field contains the email address(es) of the recipient(s). Multiple recipients can be specified by separating each one with a comma character.
ReplyTo <mailbox@example.com>	An optional email address where replies to this message will be directed.
CC <maibox@example.com[, mailbox@example.com]>	An optional list of carbon copy recipients of this message. Multiple carbon recipients can be specified by separating

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

	each one with a comma character.
Subject <text>	An optional subject for the message.
Header <Header: Value>	Allows you to explicitly place Header/ Value combinations into the message. This makes it possible for you to place custom or other non-standard headers into your *.raw messages.

Special Fields Supported by RAW

File attachment and encoding

```
x-flag=attach <filepath, method> [-x]
```

Example: `x-flag=attach <c:\utils\pkzip.exe, MIME> -x`

This X-FLAG specifies the value "ATTACH" along with two parameters within the <> characters. The first parameter is a complete path to the file which should be attached to the message. The second parameter which is separated from the first by a comma character and specifies the method of encoding that is to be used when attaching the message. MDaemon supports two values for this parameter. The method of MIME instructs the server to use the Internet standard Base64 method of message encoding. The method of ASCII instructs the server to simply import the file into the message. An optional -X parameter at the end of the string instructs the server to remove the file from disk once it has been attached.

Delivery Status Notification

```
x-flag=confirm_delivery
```

When converting a RAW message which contains this flag into RFC-2822 mail, the string is transformed to the "Return-Receipt-To: <sender@example.com>" construct.

Placing Specific Header/Value Combinations into the RFC-2822 Message

```
header <header: value>
```

If you wish to place a specific header/value combination into the RFC-2822 message that will be generated from a RAW file, you will need to use the HEADER macro listed in the RAW Headers section above. For example, if you want the header "Delivered-By: mail-machine@example.com" to be placed into the RFC-2822 message you would place this: "header <Delivered-By: mail-machine@example.com>" in the RAW message. Note that the "header" macro requires both the field and value. You can place as many "header" macros as you need into a RAW message.

DKIM Signing RAW Messages

```
x-flag=sign
```

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Including this special command in a *.raw file will cause the RAW message to be DKIM signed. This should only be used in RAW messages that you have configured to bypass the Content Filter (by starting their filenames with "p" or "P"). You should not use this command in normal RAW Messages that are processed through the filter. Those messages will be signed normally.

All RAW messages that are generated by the Content Filter will use the x-flag=sign command automatically.

Sample RAW mail messages

Sample 1:

```
from <mdaemon@altn.com>
to <user01@example.com>

Hello John!
```

Sample 2:

```
from <user01@example.com>
to <user09@example.net>
subject <Requested Files>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\docs\files\data01.zip, MIME> -X

Here are all those files you asked for.
```

8.4 Semaphore Files

MDaemon is equipped with support for Semaphore Files, which can be used for a variety of purposes, including causing MDaemon to perform specific actions. Periodically MDaemon will scan the \APP\ subfolder for the existence of these files. If it finds one, the associated behavior is triggered and the semaphore file is removed. This provides for a simple mechanism that enables administrators and developers to manipulate MDaemon without actually handling the interface. The following is a list of the semaphores and what they do:

FILENAME	ACTION
ACLFIX.SEM	Runs the ACL file cleanup routine.
ADDUSER.SEM	This semaphore creates new accounts. It is used to force MDaemon to append new records to the end of the USERLIST.DAT file without causing a potentially time consuming complete rebuild of the user database.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

	Each line in this file must be a complete account record of the form specified in the Account Management Functions section of the MDaemon API (see `MD-API.html` in MDaemon's `\docs\API\` subfolder). Multiple new accounts can be specified – one account record per line. MDaemon will process the file one line at a time and add each new account. You can create `ADDUSER.LCK` to lock the file while you are updating it and MDaemon will not touch `ADDUSER.SEM` until `ADDUSER.LCK` is deleted. To see a sample `ADDUSER.SEM` file open `ADDUSER.SMP` in your APP directory with a text editor.
`ALERT.SEM`	Displays in a pop-up window the contents of the semaphore file to all WorldClient users who are logged in when the file is created. It is not, however, displayed to all users immediately—it is displayed to each user individually the next time his or her browser makes a request to the WorldClient server. **Note:** Unlike other semaphore files, this file is WorldClient specific. Instead of placing it in the `\app\` directory it must be placed in the `\MDaemon \WorldClient\` directory.
`ALIAS.SEM`	Reloads aliases data file(s).
`AUTORESPEXCEPT.SEM`	Reloads the Autoresponder exception file(s).
`BATV.SEM`	Reloads Backscatter Protection (BATV) data file(s).
`BAYESLEARN.SEM`	This SEM manually starts the Bayesian learning process. This is like clicking the Learn button on the Bayesian tab of the Spam Filter. Note: this will start the Bayesian learning procedure even if you have Bayesian learning disabled.
`BESBACKUP.SEM`	This SEM initiates a backup of the BlackBerry Enterprise Server database, exactly like clicking the *Backup BlackBerry Enterprise Server database files* button at: BlackBerry Enterprise Server » Backup/ Restore 329.
`BESSLOWSYNC.SEM`	Start a BlackBerry Enterprise Server (BES) slow sync operation.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

BLACKLIST.SEM	Reloads the blacklist data files.
CATLIST.SEM	Reloads the internal cache of Catalog names.
CFILTER.SEM	Reloads Content Filter rules, clears Content Filter cached data, reloads the Spam Filter's White List (no filtering) 416 file.
CLEARQUOTACOUNTS.SEM	The results of user quota checks are maintained in the quotacounts.dat file. If you wish to clear the cached quota value for a user, add the user's email address to this SEM file and then place it in the \app\ folder. If an asterisk (*) is on a line by itself, the entire file will be deleted thereby invalidating all cached quota counts.
DELUSER.SEM	You can use this semaphore file to delete one or more user accounts. Create a text file containing the addresses of each account that you want to be deleted (one address per line), name the file DELUSER.SEM and then move it to MDaemon's \app\ directory. MDaemon will delete the accounts and then delete the DELUSER.SEM file.
DNS.SEM	Reloads the Windows DNS servers 58 and the Spam Filter's DNS settings.
DOMAINSHARING.SEM	Reloads domain sharing data file.
DYNAMICSCREENUPD.SEM	Adds entries to the DynamicScreen.dat file. Place the desired entries into this file and then MDaemon will manage adding them to the the DynamicScreen.dat file in the proper manner.
EDITUSER.SEM	This semaphore is used to update specific records within the USERLIST.DAT file without a potentially time consuming complete rebuild. To update a specific record within USERLIST.DAT you first construct a complete replacement record according to the format specified in the Account Management Functions section of the MDaemon API (see MD-API.html in MDaemon's \docs\API\ subfolder). The new record will reflect the changes that need to be updated within USERLIST.DAT. How does MDaemon know which record in USERLIST.DAT to update? This is accomplished by prepending the new record with the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

	original record's email address followed by a comma. The EDITUSER.SEM file can contain multiple records to update – each on its own line. MDaemon will process the file one line at a time. You can create EDITUSER.LCK to lock the file while you are updating it and MDaemon will not touch EDITUSER.SEM until EDITUSER.LCK is deleted. To see a sample EDITUSER.SEM file open EDITUSER.SMP in your \APP\ directory with a text editor.
EXITNOW.SEM	Shuts down MDaemon.
GATEWAYS.SEM	For optimal performance, MDaemon keeps its list of gateways in memory. Create a GATEWAYS.SEM in MDaemon's APP directory for it to reload the gateways.dat file.
GREYLIST.SEM	Reloads Greylisting data file(s).
GROUPS.SEM	Reloads account grouping data file(s).
GRPLIST.SEM	Reloads the internal cache of Mailing List names.
HANGUPG.SEM	Forces a conditional hang-up of RAS device. MDaemon will wait for any pending mail sessions to close and will then hang-up the RAS session.
HANGUPR.SEM	Forces unconditional hang-up of RAS device. This is an immediate and unconditional hang-up without regard to mail sessions which may be in progress across the connection.
HOSTSCREEN.SEM	Reloads Host Screen data file(s).
IPSCREEN.SEM	Reloads IP Screen data file(s).
IPSHIELD.SEM	The IPShield.dat file is cached in memory to increase access speed. Use IPSHIELD.SEM to reload the file into memory
LDAPCACHE.SEM	Reloads LDAP and gateway user data file(s).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

LOCKSEMS.SEM	Prevents all semaphore file processing until user removes it.
LOGSETTINGS.SEM	Reloads log file settings.
MDSPAMD.SEM	Reloads the Spam Filter white list and MDSPAMD, which forces it to reinitialize all its configuration data.
MINGER.SEM	Stops and then restarts the Minger 640 server.
MXCACHE.SEM	Reloads MX Cache data file(s).
NODNSBL.SEM	Reloads DNSBL white list file.
NOPRIORITY.SEM	Forces MDaemon to reload the NoPriority.dat file.
ONLINE.SEM	MDaemon will create this semaphore file once it makes a successful connection using RAS to the ISP. MD will remove the semaphore once the connection has been terminated. This is useful if you want to know when MD is using the RAS sub-system.
POSTDIAL.SEM	MDaemon will create this file immediately after a connection made by MDaemon is taken down.
PREDIAL.SEM	MDaemon will create this file just before trying to use RAS/DUN. This will allow other software to detect when it should free the dialup port so that MDaemon can use it.
PRIORITY.SEM	Reloads Priority mail data file(s).
PROCBAD.SEM	Initiates delivery of Bad Queue content.
PROCDIG.SEM	Initiates construction and delivery of mailing list digests.
PROCHOLDING.SEM	Initiates delivery of Holding Queue content.
PROCNOW.SEM	Initiates a check for remote mail and delivery of queued remote mail.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

PROCREM.SEM	MDaemon will immediately go into mail processing mode and transact all remote mail.
PROCRETR.SEM	Initiates delivery of Retry Queue content.
PRUNE.SEM	Reloads auto-pruning settings.
PUBLICSUFFIX.SEM	Reloads the Public Suffix 468 file.
QUEUE.SEM	This semaphore file is used to enable/disable the mail queues. The file can contain any number of lines but each one has to contain one of the following strings (one per line): ENABLE INBOUND, ENABLE REMOTE, ENABLE LOCAL, or DISABLE INBOUND, DISABLE REMOTE, DISABLE LOCAL.
QUEUERUN.SEM	Just before a mail session begins MDaemon will create this semaphore file. Inside the file will be a datestamp indicating the time and date of the most recent mail processing interval.
RESTART.SEM	Stops and then starts MDaemon.
RESTARTCF.SEM	Stops and restarts CFEngine.exe (the Content Filter executable).
RESTARTWC.SEM	Stops and restarts WorldClient. This only works when WorldClient is running using its own built-in web server 229.
RELOADCACHE.SEM	Reloads all cached data settings and files except for Content Filter settings and files.
REVERSEEXCEPT.SEM	Reloads reverse lookups exception file.
SCHEDULE.SEM	Reloads schedule data file(s).
SPAMHONEYPOTS.SEM	Reloads spam honeypots data files(s)
SPF.SEM	Reloads SPF, DKIM, and VBR data files(s).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

SUPPRESS.SEM	Reloads black list settings and clears cached domain settings.
TARPIT.SEM	Reloads tarpit and dynamic screening data file(s).
TRANSLAT.SEM	Reloads the header translation data files.
TRAY.SEM	Redraws MDaemon's icon in the system tray.
TRUST.SEM	Trusted domains and IP addresses are kept memory resident for optimal performance. If you need to reload these settings manually you can create TRUST.SEM to do it.
UPDATEAV.SEM	Initiates antivirus definition update.
UPDATESA.SEM	Initiates a Spam Filter update.
USERLIST.SEM	Reload the USERLIST.DAT file. Use this when you make modifications to the USERLIST.DAT and need MDaemon to reload it.
WATCHDOG.SEM	MDaemon will check for and remove this semaphore from the APP directory at approximately 10-20 second intervals. This file can be used by external apps to check if MDaemon is running. If this file remains in the APP directory for more than 20 seconds, that is a good indication that MDaemon is no longer running.

8.5 Route Slips

A message file waiting in a queue typically contains within its headers all the information that is needed to get the message delivered to the proper location. There are headers stored within the file (such as the X-MDaemon-Deliver-To header) which provide MDaemon with instructions as to where and to whom the message should be delivered. Sometimes however it is necessary or useful to override this information and provide specific alternatives to where and to whom a message must be sent. Route Slips provide just such a mechanism. A route slip is a file that provides MDaemon with very specific instructions as to where and to whom a message should be sent. If a route slip is present for a particular message file then the settings within the route slip, and not those within the .MSG file itself, control where and to whom the message is

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

sent.

Route slips end with the extension .RTE. For example, if a message file waiting to be sent is called "MD0000.MSG," then the corresponding route slip file for this message will be called MD0000.RTE and must be located in the same folder (mail queue) as the message file.

The format of a route slip is as follows:

```
[RemoteHost]
DeliverTo=example.net
```

This section of a route slip provides MDaemon with the server to which the corresponding .MSG file is to be sent. MDaemon will always attempt a direct connection to this host attempting to route the message in as short a time as possible. Only one host may be specified.

```
[Port]
Port=xxx
```

This switch specifies the port that the TCP/IP connection and delivery attempt should be made on. Port 25 is the default for SMTP email.

```
[LocalRcpts]
Rcpt0=address@example.com
Rcpt1=other-address@example.com
Rcpt2=yet-another-address@example.com

[RemoteRcpts]
Rcpt0=address@example.net
Rcpt1=other-address@example.net
Rcpt2=yet-another-address@example.net
```

These sections of the route slip allow you to specify any number of local and remote recipients who should receive a copy of the associated .MSG file. Local and remote recipient addresses must be kept separate and placed in their corresponding [LocalRcpts] and [RemoteRcpts] sections.

Route slips provide a good mechanism for delivering or redirecting email but they are not generally necessary. One use that MDaemon makes of route slips is in the case of "routed" mailing list mail. When you have a mailing list that is set to route a single copy of the list message to some remote host, a route slip is employed to accomplish this. It is a very efficient method of mail delivery when you have bulk addresses to deliver mail to since only a single copy of the message is required while any number of recipients of the message can be specified. Not all remote hosts allow this sort of routing to occur however. Since it is ultimately they who will have to deliver a copy of the message file to each address, some hosts place an upper limit on the number of recipients they will allow you to specify.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

8.6 MDaemon and Proxy Servers

MDaemon was purposely designed to be highly versatile. Consequently, it can be configured for use with a wide variety of network configurations and various other products, and its flexibility allows it to work well with LAN proxy servers. To configure MDaemon to work through any proxy server, all you must do is make sure that the port settings (see Ports 561) you are using do not conflict with any that may be set in the proxy server itself. For example, SMTP email normally takes place on port 25. Since an IP address can only have a single port 25, two servers cannot both listen for SMTP email at the same time on the same machine. When attempting to integrate MDaemon with a proxy, it is recommended that you allow MDaemon as much control over mail processing and delivery as possible. To that end, SMTP, POP, IMAP, and several other ports in the proxy may need to be disabled so that MDaemon can handle mail delivery independently.

However, should you find it necessary to channel mail through a proxy, MDaemon allows you to configure the ports which it will use to send and receive SMTP/POP/IMAP transactions. You may need to set these ports to non-standard values in order to filter your SMTP/POP/IMAP transactions through a proxy server or firewall.

For more detailed information on configuring MDaemon to work with a proxy server, please consult the support resources available at: www.altn.com.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Section

9 Glossary

ACL—Stands for **A**ccess **C**ontrol **L**ists. ACL is an extension to the Internet Message Access Protocol (IMAP4) that makes it possible for you to create an access list for each of your IMAP message folders, thus granting access to your folders to other users whom also have accounts on your mail server. Further, you can set permissions governing the extent to which each user has control over those folders. For example, you can designate whether or not a user is allowed to delete messages, flag them as read or unread, copy messages to folders, create new subfolders, and so on. Only email clients that support ACL can be used to share this access and set permissions. However, if your email client doesn't support ACL you can still set these permissions from the MDaemon interface.

ACL is fully discussed in RFC 2086, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2086.txt

ASCII—Pronounced as-key, ASCII is an acronym for "**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange". It is the worldwide standard code for representing all upper and lower-case Latin letters, numbers, and punctuation as a 7 digit binary number, with each character assigned a number from 0 to 127 (i.e. 0000000 to 1111111). For example, the ASCII code for uppercase M is 77. The majority of computers use ASCII codes to represent text, which makes it possible for them to transfer data to other computers. Most text editors and word processors are capable of storing files in ASCII format (sometimes called ASCII files). However, most data files—particularly those containing numeric data—are not stored in ASCII format.

Several larger character sets have 128 additional characters because they use 8 bits instead of 7. These extra characters are used to represent symbols and non-English characters. The DOS operating system uses a superset of ASCII called extended ASCII or high ASCII. A standard that is closer to universal, however, is ISO Latin 1, which is used by many operating systems and Web browsers.

ATRN—See ETRN and ODMR below.

Attachment—A file attached to an email message. Most email systems only support sending text files as email, therefore if the attachment is a binary file or formatted text file (e.g. a word processor document), it must first be encoded as text before it is sent and then decoded once it is received. There are a number of encoding schemes—two of the most prevalent being Multipurpose Internet Mail Extensions (MIME) and Unix-to-Unix encode (Uuencode). For incoming messages, Alt-N's MDaemon server can be configured to either leave the decoding process to the recipient's email client or automatically decode attachments and store them in a specific location before delivering the message to the local user.

Backbone—A line or series of connections that form the major pathway within a network. This term is relative since the non-backbone lines in a large network might be larger than the backbone in a smaller network.

Bandwidth—The amount of data that can be transmitted in a fixed amount of time through a network or modem connection, usually measured in bits-per-second (bps).

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

A full page of English text is about 16,000 bits, which a fast modem could transfer in about 1 to 2 seconds. Full-motion full-screen video would require roughly 10,000,000 bits-per-second, depending on compression.

A good illustration of bandwidth is a highway. The highway represents the connection while the cars traveling on it represent the computer data. The wider the highway (the greater the bandwidth) the more cars that will be able to travel on it.

Baud—Baud rate is a measure of how frequently carrier signals change value on a phone line. It is a reference to the speed at which a modem transmits data. Usually, slower modems are described in terms of Baud rate while higher speed modems are described in bits per second. "Baud rate" and "bits per second" are not necessarily synonymous terms since each signal can encode more than one bit in high-speed connections.

Bit—A single **B**inary dig**it**. It is the smallest unit of computer data; a single digit number in base-2 (i.e. 0 or 1). It is usually abbreviated with a lower case "b" as in "bps" (bits per second). A full page of text is approximately 16,000 bits.

Bitmap—Most pictures you see on your computer, including all the ones found on the Internet, are bitmaps. A bitmap is a really just a map of dots (or bits) that looks like a picture as long as you're not to close to the screen, or have the bitmap magnified too much, to see the shape they make. Common Bitmap file types include BMP, JPEG, GIF, PICT, PCX, and TIFF. Because bitmap images are made up of a bunch of dots, if you zoom in on a bitmap it looks blocky rather than smooth. Vector graphics (usually created in CorelDraw, PostScript, or CAD formats) scale up much better because they are geometric shapes generated mathematically rather than simply being made of seemingly "random" dots.

Bps—"**B**its **P**er **S**econd" is a measurement of how fast computer data can be moved from one place to another. For example, a 33.6 kbps modem can transfer 33,600 bits per second. Kilobits (1000 bits) per second and megabits (1.000,000 bits) per second are abbreviated "Kbps" and "Mbps" respectively.

Browser—Short for "Web browser", it is an application used to display web pages. It interprets HTML code, text, hypertext links, images, JavaScript, and so on. The most widely distributed browsers are Internet Explorer and Netscape Communicator.

Byte—A set of bits (usually eight) that represent a single character. There are 8 bits in a byte, sometimes more, depending on how the measurement is being made. "Byte" is abbreviated with an uppercase "B".

Cache—Pronounced like "cash". There are various types of caches, but all are used to store recently used information so that it can be accessed quickly later. For example, a web browser uses a cache to store the pages, images, URLs, and other elements of web sites that you have recently visited. When you return to a "cached" page the browser will not have to download these elements again. Because accessing the cache on your hard disk is much faster than accessing the Internet, this significantly speeds up browsing.

MDaemon's IP Cache stores the IP addresses of domains to which you have recently delivered messages. This prevents MDaemon from having to lookup these addresses

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

again when delivering additional messages to the same domains. This can greatly speed up the delivery process.

CGI—Common **G**ateway **I**nterface is a set of rules that describe how a Web Server communicates with another piece of software on the same machine, and how the other piece of software (the "CGI program") talks to the web server. Any piece of software can be a CGI program if it handles input and output according to the CGI standard. However, a CGI program is usually a small program that takes data from a web server and does something with it, like putting the content of a form into an email message, or doing something else with that data. CGI programs are often stored in a web site's "cgi-bin" directory and therefore appear in a URL that accesses them, but not always.

cgi-bin—The most common name of the directory on a web server in which CGI programs are stored. The "bin" part of "cgi-bin" is short for "binary" because most programs used to be referred to as "binaries". In reality, most cgi-bin programs are text files; scripts executed by programs located elsewhere.

CIDR—"**C**lassless **I**nter-**D**omain **R**outing" is a new IP addressing system that replaces the older system, which was based on classes A, B, and C. CIDR IP addresses look like normal IP addresses followed by a slash and number, called the IP prefix. For example:

123.123.0.0/12

The IP prefix defines how many addresses are covered by the CIDR address, with lower numbers covering more addresses. In the above example, the IP prefix of "/12" can be used to address 4,096 former Class C addresses.

CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

CIDR is addressed in RFCs 1517-1519, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

Client—A software program that is used to contact and obtain data from or send data to a *server* software program. The server is usually located on another computer, either on your local network or at some other location. Each *client* program is designed to work with one or more specific kinds of *server* programs, and each server requires a specific kind of client. A web *browser* is a specific kind of client that communicates with web *servers*.

Common Gateway Interface—See CGI above.

Cookie—In computer terminology, a *cookie* is data sent by a web server to your web browser, which is saved and later used for various purposes when you return to the same site or go to another location on the site. When a web server receives a request from a web browser that includes a cookie, it is able to use the information the cookie contains for whatever purpose it was designed, such as customizing what

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

is sent back to the user, or for keeping a log of the user's requests. Typically, cookies are used for storing passwords, usernames, preferences, shopping cart information, and similar things related to the site to which they correspond so that the site can appear to "remember" who you are and what you've done there.

Depending on your browser's settings, you may accept or not accept the cookies, and save them for various amounts of time. Usually cookies are set to expire after a predetermined amount of time and are saved in memory until the web browser software is closed down, at which time they may be saved to disk.

Cookies **cannot** read your hard drive. They can, however, be used to gather information about you related to your usage of their particular web sites, which would be impossible without them.

Dial-up Networking—A component in Windows that enables you to connect your computer to a network via a modem. Unless your computer is connected to a Local Area Network (LAN) with access to the Internet, you will need to configure Dial-Up Networking (DUN) to dial a Point of Presence (POP) and log on to your Internet Service Provider (ISP) before you will have Internet access. Your ISP may need to provide certain information, such as the gateway address and your computer's IP address.

DUN is accessed through the My Computer icon. A different dialup profile can be configured for each online service that you use. Once configured, you can copy a profile shortcut to your desktop so that all you need to do to make a connection is double-click the connection icon.

Default—This term is used to refer to the preset value for options in computer programs. Default settings are those settings which are used when no specific setting has been designated by the user. For example, the default font setting in Netscape Communicator is "Times". This setting will remain "Times" unless you change it to something else. Default settings are usually the value that most people will choose.

Frequently the term *default* is also used as a verb. If a custom setting won't work or the program lacks some needed bit of data for completing a task, it will usually "default" to a specific setting or action.

DHCP—An acronym for "**D**ynamic **H**ost **C**ontrol **P**rotocol". Network servers use this protocol to dynamically assign IP addresses to networked computers. A DHCP server waits for a computer to connect to it and then assigns it an IP address from a stored list.

DHCP is addressed in RFC-2131, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2131.txt

Domain Gateway—See Gateway below.

Domain Name—This is the unique name that identifies an Internet web site. For example, "altn.com" is the domain name of Alt-N Technologies. Each domain name contains two or more parts separated by dots; the leftmost part is the most specific while the rightmost part is the most general. Each domain name also points to the IP address of a single server, but a single server may have more than one domain

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

name. For example, "mail.altn.com", "alt-n.com", and "example.com" could all point to the same server as "altn.com", but "altn.com" could not point to two different servers. There are, however, methods for designating alternate servers to which clients will be directed if the main server goes down or is otherwise unavailable.

It is also common for a domain name to be registered but not be connected to an actual machine. The usual reason for this is the domain name's owner hasn't created a web site yet, or so that they can have email addresses at a certain domain without having to maintain a web site. In the latter case, there must be a real Internet machine to handle the mail of the listed domain name.

Finally, it is common to see the term "domain name" shortened and referred to as simply "domain". The word "domain" has other meanings and can refer to other things, such as a Windows NT domain or a class of values, so you should be aware of the distinction in order to avoid confusion.

Domain Names are addressed in RFCs 1034-1035, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1034.txt

http://www.rfc-editor.org/rfc/rfc1035.txt

DomainPOP—Developed by Alt-N Technologies to be a part of the MDaemon server, DomainPOP makes it possible to provide email services for an entire LAN or workgroup from a single ISP POP mailbox. In the past, unless a company's email server had on constant "live" connection to the Internet, the only way to provide Internet email services to a workgroup was for each person to have their own mailbox on the company's ISP from which they could collect their mail. With DomainPOP only a single mailbox is required. The ISP pools all mail for the company's domain name into the mailbox from which it is periodically collected by DomainPOP. Then, DomainPOP parses the messages to determine the intended recipients of each and distributes them to the appropriate local user mailboxes. Thus email is provided for an entire network from a single dialup ISP account.

Download—The process by which your computer retrieves or obtains data from another computer. For example, information is obtained from the Internet by *downloading* it from other computers. The reverse of this is *uploading*. If you wish to send information to another computer then you will *upload* it to them.

Driver—A small program that communicates with a certain hardware device. Drivers contain information needed by the computer and other programs to control and recognize the device. Windows-based computers often have drivers packaged as a dynamic link library (DLL) file. Most hardware devices used with Macs do not need drivers, but when a driver is necessary it will usually come in the form of a System Extension.

DUN—See Dial-up Networking above.

Email—Stands for "Electronic mail". This term also appears in the forms: "E-mail", "e-mail", and "email"; all have the same meaning. Email is the transmission of text messages over communications networks. Most computer networks have some form of email system. Some email systems are confined to a single computer network, but others have gateways to other networks (which enables them to communicate with

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

multiple locations), or to the Internet (which enables them to send email anywhere in the world).

Most email systems include some form of *email client* (also referred to as a *mail client* or just *client*) which contains a text editor and other tools for composing messages, and one or more *servers* which receive the email from the clients and route it to its appropriate destination. Typically, a message is composed using the client, passed to a server for delivery to the *email address* (or addresses) specified in the message, and then routed by the server to another server that is responsible for storing messages destined for that address. If the message's destination is a local address for which the original server is responsible then it may be stored on the original server rather than routed to another. Last, the recipient of the message will connect to their server and retrieve the message by using their email client. This entire process of transferring an email message from your client to its destination server usually only takes a few seconds or minutes.

Besides containing simple text, email messages may also include file *attachments*. These attachments can be any type of file that you desire: pictures, text files, program files, other email messages, and so on. However, since most email systems only support sending text files, attachments must first be encoded (converted to a text format) before they can be sent, and then decoded when they arrive at their final destination. This process is usually done automatically by the sending and receiving mail clients.

All Internet Service Providers (ISPs) offer email. Most also support gateways so that you can exchange email with users of other email systems. Although there are many different protocols used for processing email by many different email systems, several common standards make it possible for users on virtually all systems to exchange messages.

Email Address—A name or string of characters that identifies a specific electronic mailbox on a network to which email can be sent. Email addresses are the locations to and from which email messages are sent. Email servers need email addresses so that they can route messages to their proper destinations. Different types of networks have different formats for email addresses, but on the Internet all email addresses have the form: "mailbox@example.com".

For example,

```
Michael.Mason@altn.com
```

Email Client—Also called a *mail client* (or just *client*), an *email client* is a software application that enables you to send, receive, and organize email. It is called a client because email systems are based on client-server architecture; a client is used to compose the email and then send it to a server, which then routes it to the recipient's server from which it will be retrieved by the recipient's client. Usually, email clients are separate software applications installed on the user's machine, but products such as Alt-N Technologies' WorldClient Server contain a built in client that is "served" to the user's web browser. Thus, their browser is used as the client rather than needing to install one on their machine. This greatly enhances the portability and convenience of email.

Encryption—A security measure, *encryption* is the coding or scrambling of information

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

in a file so that it will only be intelligible when it has been decoded or decrypted. Encryption is frequently used in email so that if a third party intercepted the email they would not be able to read it. The message is encrypted when it is sent and then decrypted at its final destination.

Ethernet—The most common type of connection used in a Local Area Network (LAN). Two of the most widely used forms of Ethernet are 10BaseT and 100BaseT. A 10BaseT Ethernet can transfer data at speeds up to 10 mbps (megabits per second) through a cable or wireless connection. A 100BaseT Ethernet transfers data at speeds up to 100 mbps. A Gigabit Ethernet can transfer data at rates up to 1000 mbps and is employed by some Apple computers.

ETRN—An acronym meaning **E**xtended **TURN**. It is an extension to SMTP that enables an SMTP server to send a request to another SMTP server to send, or "dequeue", mail that is being held for it. Because SMTP by itself cannot request mail (email is usually requested via the POP or IMAP protocols), this makes it possible for the SMTP server making the ETRN request to cause the remote server to start an SMTP session and begin sending the stored email to the host specified in the request.

The `TURN` command used for this purpose posed a security risk because it caused the SMTP session to reverse direction and begin sending the stored mail immediately without any verification or authentication that the requesting server was actually who it claimed to be. `ETRN` starts a new SMTP session rather than reversing direction. Thus if the server making the request is a "spoofed" host, the sending server will still attempt to deliver the mail to the real host instead. There is now a proposed standard that introduces Authenticated TURN (`ATRN`), which, like `TURN`, reverses the direction of the SMTP session but requires authentication before doing so. This new standard is On-Demand Mail Relay (ODMR). Alt-N Technologies' MDaemon server supports both ETRN and ODMR's ATRN.

ETRN is addressed in RFC 1985, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1985.txt

ODMR is addressed in RFC 2645, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2645.txt

FAQ—Pronounced together as "fack" or as separate letters "F-A-Q", FAQ stands for "**F**requently **A**sked **Q**uestions". FAQs are documents that provide answers to the most commonly asked questions on a given subject. They usually appear in some form of list format with each question listed first followed by its answer. In larger FAQs, oftentimes all of the questions will be listed at the beginning of the document with references (or hyperlinks, in online FAQs) to the location of the question and answer in the document. FAQs are frequently used as a starting point for technical support and instructions—a great deal of time and effort can be saved if you have access to a FAQ that answers your question instead of being forced to contact technical support.

File Transfer Protocol—See FTP below.

Firewall—In computer terminology, a *firewall* exists when you undertake security measures, through either software or hardware means, to separate a computer

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

network into two or more parts, or otherwise limit access to it to certain users. For example, you might want to let everyone view the home page of a web site hosted on your network but allow only your employees to get to an "employee only" area. Regardless of the method that you use to accomplish this—requiring a password, allowing connections from only certain IP addresses, or the like—the employee area is said to be behind a firewall.

FTP—Acronym for "**F**ile **T**ransfer **P**rotocol." It is a common and efficient method of transferring files via the Internet from one computer to another. There are specific client/server applications designed for this purpose called "FTP servers" and "FTP clients"—FileZilla, for example, is one of the most common clients. Usually FTP clients can perform quite a few other functions besides simply transferring files and are thus highly useful products. Some web browsers also contain support for File Transfer Protocol, though sometimes for downloading only. Additionally, most FTP servers are "anonymous FTP", which means that anyone can log in to them in order to download files—usually by specifying "anonymous" as the user name and then your email address as the password. Oftentimes you can download files from anonymous FTP sites without having to log in at all—they can be retrieved by simply clicking on a link. For browsers that support FTP, usually all that needs to be done is to connect to the FTP site using "ftp://..." in its URL rather than "http://..."

FTP is addressed in RFC-959, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc959.txt

Gateway—Computer hardware or software that translates data between two applications or networks with protocols that are dissimilar. "Gateway" is also used to describe any means by which access is provided from one system to another. For example, your ISP is a gateway to the Internet.

Alt-N Technologies' MDaemon Messaging Server can function as an email gateway for other domains through the use of its Domain Gateways feature. It acts as an intermediary, or Gateway, by collecting the domain's email and then holding it until the domain collects it. This is useful both for domains that do not maintain a continuous connection to the Internet and for domains that require a backup server in case theirs goes down.

GIF—"**G**raphics **I**nterchange **F**ormat" is a popular format for image files and is the most common format of images found on the Internet. GIF uses indexed colors or a palette of a certain number of colors, which greatly reduces file size—especially when the image contains large areas of the same color. The reduced size enables them to be quickly transferred between systems and accounts for their popularity on the Internet. The GIF compression formula was originally developed by CompuServe and thus you will often see GIF referred to as CompuServe GIF.

Graphical User Interface—See GUI below.

GUI—Pronounced "gooey", this acronym stands for "**G**raphical **U**ser **I**nterface". A GUI makes it possible to interact with your computer or application by using a pointing device to click graphical elements on the screen rather than typing in text at a command line. The Microsoft Windows and Apple Mac operating systems are both GUI-based, but—although first introduced by Apple—the idea of a graphical user interface actually originated from Xerox.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Host—Any computer on a network that acts as a server for other computers on the same network. The host machine may be running a web server, email server, or other services, and it is common for it to provide several services at once. Host is also often used in the verb form "to host". For example, a machine running an email server would be "hosting" the email.

On peer-to-peer networks it is common for machines to be both hosts and clients at the same time. For example, your machine may host your network's printer but also be used by you as a client to collect email and download files from another host.

HTML—An acronym for "**H**ypertext **M**arkup **L**anguage. It is the coding language used to create Hypertext documents used on the World Wide Web. Simply put, an HTML document is a plain text document that contains formatting codes and tags that the user's web browser interprets and presents as a web page complete with formatted text and colors. For example, a browser receiving an HTML document containing the text "<B>Text</B>" would present the word "Text" in Bold. Because plain text files are very small, this makes it possible for them to be quickly transferred over the Internet.

HTTP—Hyper**t**ext **T**ransfer **P**rotocol (HTTP) is the protocol used for transferring *hypertext* files between computers over the Internet. HTTP requires a client program on one end (usually a web browser) and an HTTP server on the other end.

HTTP is addressed in RFC-2616, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2616.txt

Hypertext—Any text that contains a hyperlink or jump to another document or place within the same document is called hypertext. Sometimes the text is also called a hypertext link or simply link. Hypertext can be either a word or phrase and has the link embedded in it so that clicking it will move you to the "book marked" location or cause the linked document to be displayed. Usually hypertext links are apparent because the text is underlined and a different color, but that is not required. Sometimes hypertext will look no different than normal text, but will almost always be indicated by some sort of graphical change to your pointer when the mouse pointer is paused over it.

Hypertext Markup Language—See HTML above.

IMAP—Developed by Stanford University, **I**nternet **M**essage **A**ccess **P**rotocol (IMAP) is a protocol used for managing and retrieving email messages. The latest version is IMAP4 and is similar to POP3 but with a number of additional features. IMAP4 is best known as a protocol used for managing email messages on the server rather than on the user's local machine—messages can be searched for keywords, organized in folders, specifically selected for downloading, and other features, all while they are still on the server. Thus IMAP places less demand on the user's machine and centralizes email so that it can be accessed from multiple locations.

IMAP is addressed in RFC-2060, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2060.txt

IMAP4 ACL extension—See ACL above.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Internet—The Internet was created in 1969 by the United States military, originally to be a communications network that couldn't be destroyed during a nuclear war. It now consists of millions of computers and networks all over the world. By design, the Internet is decentralized—it is not controlled by any company, organization, or country. Each host (or machine) on the Internet is independent of the others and can provide whatever information or services its operators wishes to make available. Nevertheless, most information transferred over the Internet at some point passes through "backbones", which are extremely high-bandwidth high-speed connections controlled by the largest Internet Service Providers and organizations. Most people access the Internet through an online service such as AOL or through an Internet Service Provider (ISP) that maintains or is connected to one of these backbones.

Many people believe that the *World Wide Web* (WWW) and the Internet are the same thing, but this is not the case. The WWW is only one part of the Internet not the Internet itself. It is the most visible and popular part, largely driven by commerce, but still only a part.

Intranet—Simply put, an intranet is a small or private Internet used strictly within a company or organization's network. Although intranets vary widely from organization to organization, they may contain any of the features available on the Internet. They may have their own email systems, file directories, web pages to be browsed, articles to be read, and so on. The primary difference between an intranet and the Internet is that an intranet is relatively small and confined to an organization or group.

IP—An acronym for "**I**nternet **P**rotocol" (e.g. as in TCP/IP). Internet protocols make it possible for data to be transferred between systems over the Internet. Regardless of each machine's platform or operating system, if the same Internet Protocol is used by each machine then they will be able to transfer data to each other. The term "IP" is also commonly used as a further abbreviation of the term "IP Address". The current standard Internet Protocol is IP version 4 (IPv4).

Internet Protocol is addressed in RFC-791, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc791.txt

IP Address—Occasionally called an IP Number, IP Address stands for **I**nternet **P**rotocol Address and is used to identify a particular TCP/IP network and the hosts or machines on that network. It is a 32-bit numeric address containing four numbers between 0 and 255 separated by dots (e.g. "127.0.0.1"). Within an isolated network, each computer must have a unique IP address, which can be assigned at random. But, every computer on the Internet must have a registered IP address to avoid duplication. Each Internet IP address can be either static or dynamic. Static addresses do not change and always represent the same location or machine on the Internet. Dynamic IP addresses change and are usually assigned by an ISP to computers that are only on the Internet temporarily—such as when a user with a dial-up account accesses the Internet. However, it is still possible for a dial-up account to have a static IP address assigned to it.

ISPs and large organizations usually attempt to acquire a range or set of IP addresses from the InterNIC Registration Service so that all clients on their network or using their service may have similar addresses. These sets are broken up into three classes: Class A, B, and C. Class A and B sets are used by very large

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

organizations and support 16 million and 65,000 hosts respectively. Class C sets are for smaller networks and support 255 hosts. Class A and B sets are now very difficult to get due to the shortage of available addresses; consequently most companies have to settle for multiple class C sets instead. Because of this IP address shortage, there is a new IP address protocol called Classless Inter-domain Routing (CIDR) that is gradually replacing the older system.

The current Internet Protocol standard, IPv4, is addressed in RFC-791, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc791.txt

IP version 6 (IPv6) is addressed in RFC-2460 at:

http://www.rfc-editor.org/rfc/rfc2460.txt

CIDR is addressed in RFCs 1517-1519 at:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

IP Number—See *IP Address* above.

ISP—An **I**nternet **S**ervice **P**rovider (ISP) is a company that provides Internet access and services to the end user. Most ISPs provide multiple Internet services to their customers, such as: WWW access, email, access to newsgroups and news servers, and so on. Typically, users will connect to their ISP via dial-up, or some other form of connection, and then the ISP will connect them to a router, which will in turn route them to the Internet backbone.

Java—Developed by Sun Microsystems, Java is a network-oriented computer programming language with syntax much like C/C++ but is structured around classes instead of functions. In Internet applications it is commonly used for programming applets, which are small programs embedded in web pages. These programs can be automatically downloaded and executed by a user's browser in order to provide a large number of functions that wouldn't ordinarily be possible with just HTML or other scripting languages, and without fear of viruses or harm to your computer. Because Java is both efficient and easy to use, it is becoming popular among many software and hardware developers.

JavaScript—Not to be confused with Java, JavaScript was developed by Netscape as a scripting language designed to extend the capabilities of HTML and create interactive web pages. It is a highly pared down and easy to use programming language, which makes it much easier to use than Java and other languages but also limits it to some degree. It spite of its limitations it is very useful for adding a number if interactive elements to web sites. For example, JavaScript is useful when you want data to be preprocessed before it is submitted to the server, or when you want your pages to respond to user interaction with links or form elements. It can also be used to control plug-ins and applets based on user choices, and to accomplish a large number of other functions. JavaScript is included within the text of HTML documents and is interpreted by web browsers in order to perform the

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

functions.

JPEG—A graphics file format that is very efficient at compressing high-color and photographic images—much more so than the GIF format. While GIF is the best choice for images containing regular shapes and large areas of repeating color patterns, JPEG is much more suited to images with irregular patterns and large numbers of colors. JPEG is the most commonly used format for high-color and photographic images on the Internet. The acronym JPEG stands for "**J**oint **P**hotographic **E**xperts **G**roup"—the group that developed the format.

Kbps—Commonly used when referring to modem speeds (e.g. 56 Kbps), this acronym stands for "**K**ilo**b**its **P**er **S**econd". It is the number of kilobits (1000 bits) of data being moved or processed every second. Note that this is kilo*bits* not kilo*bytes*—a kilobyte would be eight times more data than a kilobit.

Kilobyte—A kilobyte (K or KB) is a thousand bytes of computer data. Technically it is 1024 bytes (2^10 = 1024) but in normal usage it is usually rounded off to 1000 for simplicity.

LAN—A **L**ocal **A**rea **N**etwork (LAN) is a computer network limited to a single building or area, usually having all nodes (computers or workstations) connected together with some configuration of wires or cables or some other form of media. Most large companies have a LAN, which greatly simplifies the management and sharing of information amongst employees and offices. Most LANs utilize some form of email or chat system, and share devices such as printers in order to avoid having to have a separate device for each station. When the network's nodes are connected together via phone lines, radio waves, or satellite links it is called a Wide Area Network (WAN) instead of LAN.

Latency—The time it takes a data packet to move across a network connection. While a data packet is being sent, there is "latent" time during which the sending computer waits for a confirmation that the packet has been received. In addition to bandwidth, latency is one of the factors that determine the speed of your connection.

LDAP—Lightweight **D**irectory **A**ccess **P**rotocol (LDAP) is an online directory service protocol that is a simplification of Directory Access Protocol (DAP). The directory system is in a hierarchical structure consisting of the following levels: The "root" or starting directory, country, organization, organizational unit, and individual within that unit. Each LDAP entry is a collection of attributes with a unique identifier, called a distinguished name (DN). Because it is an open protocol, is efficient, and has the ability to be distributed across many servers, LDAP may eventually make it possible for virtually any application on any platform to access directory information for locating email addresses, organizations, files, and so on worldwide.

LDAP is addressed in RFC-2251, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2251.txt

Link—See *Hyperlink* above.

List server—A server application that is used to distribute email messages to multiple recipients by simply addressing the message to a single address. Simply put, when

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

an email message is addressed to a *mailing list* maintained by the list server it will be automatically broadcast to the members of the list. Mailing lists typically have a single normal email address (for example, listname@example.com) but that address refers to a whole list of recipients rather than to a specific person or mailbox. When someone *subscribes* to a mailing list, the list server will automatically add the address to the list and distribute future emails directed to the list to that address, or member, and all other members. When someone unsubscribes, the list server simply removes the address so that it will receive no further list messages.

Frequently the term listserv is used generically to refer to any mailing list server. However, Listserv® is a registered trademark of L-Soft international, Inc. and is a specific program developed by Eric Thomas for BITNET in 1986. Besides other list servers, Alt-N Technologies' MDaemon server is equipped with an entire suite of list server, or mailing list, functions and features.

Logon—a unique code or series of characters used to gain access or otherwise identify yourself to a server or machine. In most cases a password must accompany the logon in order to gain access.

There are many terms used synonymously with "logon", such as *login*, *username*, *user name*, *user ID*, *sign-in*, and others. Frequently, "logon" is also used as a verb. For example, "I am going to *logon* to the mail server". In that context, however, the more common usage (and perhaps more proper) is "I am going to *log on* to the mail server".

Mailbox—An area in memory or on a storage device that is assigned to a specific email address and where email messages are stored. In any email system, each user has a private mailbox in which messages are stored when that user's mail server receives them. It is also common for the term "mailbox" to be used when referring to the leftmost portion of an email address. For example, "user01" in "user01@example.com" is the mailbox while "example.com" is the domain name.

Mailing List—Also called email groups, a mailing list is a list or group of email addresses identified by a single email address. For example, "listname@example.com". Typically when a list server receives an email message addressed to one of its mailing lists that message will be automatically distributed to all of the list's members (i.e. the addresses included in the list). Alt-N Technologies' MDaemon server is equipped with an extensive suite of mailing list features that enable lists to be public or private (anyone can post or join, or only members can post or join), moderated (each message must be approved by someone before it will go to the list), sent in digest format or as individual messages, and used in a variety of other ways.

Megabyte—Though technically 1,048,576 bytes (or 1024 kilobytes), a megabyte is more commonly rounded off and used to refer to a million bytes. Megabyte is abbreviated: "MB", as in "20 MB".

MIME—Defined in 1992 by the Internet Engineering Task Force (IETF), **M**ultipurpose **I**nternet **M**ail **E**xtensions (MIME) is the standard encoding method used for attaching non-text files to standard Internet email messages. Because typically only plain text files can be transferred via email, non-text files must first be encoding into a plain text format and then decoded after reaching their destination. Thus, an email program is said to be MIME Compliant if it can both send and receive files using the MIME standard. When a MIME-encoded message attachment is sent, generally both

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

the type of file being sent and the method that should be used to turn it back into its original form are specified as part of the message. There are many predefined MIME content types, such as "image/jpeg" and "text/plain". However, it is also possible to define your own MIME types.

The MIME standard is also used by web servers to identify the files they are sending to web browsers. Because web browsers support various MIME types, this enables the browser to display or output files that are not in HTML format. Further, by updating the browser's lists of MIME-Types and the software used for handling each type, new file formats can be readily supported.

MIME is addressed in RFCs 2045-2049, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2045.txt

http://www.rfc-editor.org/rfc/rfc2046.txt

http://www.rfc-editor.org/rfc/rfc2047.txt

http://www.rfc-editor.org/rfc/rfc2048.txt

http://www.rfc-editor.org/rfc/rfc2049.txt

Mirror—A server (usually an FTP server) that has a copy of the same files that are on another server. Its purpose is generally to provide an alternate location from which the mirrored files can be downloaded should the original server go down or be overloaded. The term "mirror" can also refer to a configuration whereby information is written to more than one hard disk simultaneously. This is used as a redundancy measure so that if one disk fails the computer can continue to operate without losing any vital data.

Modem—An acronym derived from **mo**dulator-**dem**odulator. A modem is a device connected to a computer that enables the transfer of data to other computers over telephone lines. The modem converts the computer's digital data to an analog format (modulates) and then transmits it to another modem where the process is reversed (demodulates). Put simply, a modem is an analog-to-digital and digital-to-analog converter. The speed at which the data is transferred is expressed in either baud-rate (e.g. 9600 baud) or kilobits per second (e.g. 28.8 kbps).

MultiPOP—A component of Alt-N Technologies' MDaemon Messaging Server that can be configured to collect email, via the POP3 protocol, simultaneously from various email servers on behalf of MDaemon's users. This makes it possible for MDaemon account holders who have email accounts elsewhere on other email servers to have that email collected and pooled with their MDaemon account email. Thus storing all of their email in a single mailbox.

NAT—See Network Address Translation below.

Network—Two or more computers connected together in some fashion. The purpose of a network is to enable the sharing of resources and information between multiple systems. Some common examples are: multiple computers sharing printers, DVD-ROM drives, hard disks, individual files, and so on.

There are many types of networks, but the most broadly defined types are Local

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Area Networks (LANs) and Wide Area Networks (WANs). In a LAN, the individual computers (or nodes) are geographically close together—usually in the same building. They are also usually connected together directly with wires, although wireless connections are becoming common as well. The nodes in a WAN are usually farther apart (in another building or city) and connected via telephone lines, satellite hook-up, or some other form of connection.

The Internet itself is a network. It is often described as a network of networks.

Network Address Translation—Network address translation (NAT) is a system whereby two sets of Internet Protocol addresses (IP addresses) are used by a single network —one for external traffic and the other for internal traffic. This is mainly used as a firewall measure to help ensure network security. Your computer will appear to have a certain IP address to computers outside your LAN while your actual IP address is altogether different. Hardware or software placed "between" your network and the Internet performs the translations between the two addresses. Using this method, it is common for multiple computers in a LAN to "share" one company IP address. Thus there is no way for someone outside your network to know your actual address and directly connect to your computer without it first being qualified or authenticated during the translation.

Network Interface Card—A network interface card (NIC) is a computer circuit board that enables a computer to be connected to a network. NICs provide a full-time network connection whereas a modem (used by most home computers to dial-in to a network via telephone lines) usually provides only a temporary connection. Most NICs are designed for specific types of networks and protocols, such as Ethernet or token ring and TCP/IP.

Network News Transfer Protocol—See NNTP below.

NIC—See Network Interface Card above.

NNTP—Network **N**ews **T**ransfer **P**rotocol (NNTP) is the protocol used to transfer and distribute messages on USENET newsgroups. The most common and popular browsers and email clients now have NNTP clients built-in.

NNTP is addressed in RFC-977, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc977.txt

Node—Any single computer connected to a network.

ODMR—On-**D**emand **M**ail **R**elay is a new protocol designed to enable mail servers with only an intermittent connection to a service provider, and which do not have a static IP address, to receive mail similarly to those servers that do have one and use the ETRN command. If the system has a static IP address, the ESMTP ETRN command can be used. However, systems with dynamic IP addresses have no widely deployed solution. ODMR solves this problem. Among other things, ODMR introduces the Authenticated TURN command (ATRN) which causes the flow of an SMTP session to be reversed (like the older TURN command) but with the added security of requiring that the requesting server be authenticated. This makes it possible for an SMTP server with a dynamic IP address to connect to its ISP and have one or more host's email delivered to it via SMTP rather than collect it via POP or IMAP. This

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

helps meet the widespread demand for a low-cost solution for those companies that need to their own mail server but cannot afford a static IP address or dedicated online presence.

ODMR is addressed in RFC 2645, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2645.txt

OEM—Original **E**quipment **M**anufacturer (OEM) is an often confusing and misunderstood term. An OEM is a company that uses another company's equipment or products in its own product that is packaged and sold under a different brand or company name. For example, HyperMegaGlobalCom, Inc. is an OEM because it purchases computer components from one or more different companies, puts them all together into a single customized product, and then sells it with "HyperMegaGlobalCom" stamped on it. The company that sold HyperMegaGlobalCom the components might also be an OEM if they in turn got their components from someone else as well. "OEM" is an unfortunate misnomer because OEMs are not actually the original manufacturers; they are the "packagers" or "customizers". In spite of this, many people still often use the term "OEM" when referring to the actual hardware manufacturers instead of those who repackage it—and understandably so.

On the fly—The term "on the fly" is commonly used it two different ways. First, it is often used to denote something that can be done "in a hurry" or easily while "in the middle" of performing some other task. For example, a bookkeeping product might support creating accounts "on the fly" while in the middle of entering sales figures —"Simply stop entering figures, click button X, enter a name, and then continue entering more figures." The other way that "on the fly" is used is in referring to something that can be generated dynamically or automatically instead of manually or statically. For example, by using the information stored in a "cookie" a customized web page might be generated "on the fly" when a user returns to a web site. Rather than requiring someone to manually create a page customized to the user's tastes, it would be generated dynamically based upon that person's actions while browsing.

Original Equipment Manufacturer—See OEM above.

Packet—A unit of computer data sent over a network. Any time you receive data from another computer on your LAN or over the Internet it comes to your computer in the form of "packets". The original file or message is divided into these packets, transmitted, and then recombined at the destination. Each packet contains a header containing its source and destination, a block of data content, and an error-checking code. It is also "numbered" so that it can be connected to related packets being sent. The process of sending and receiving packets is known as "packet-switching". Packets are also commonly called "datagrams".

Packet Switching—The process of sending and receiving packets over a network or the Internet. In contrast to circuit switching (such as in an analog telephone), which sends the data in a continuous stream over a single path or circuit, packet switching transmits the data broken up into "packets", which may not necessarily take the same route to get to their destination. Further, because the data is in separate units, multiple users can send different files simultaneously over the same path.

Parameter—A parameter is a characteristic or value. In computing, it is any value

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

passed to a program by a user or another program. Your name and password, a preference setting, font size, and so on are all parameters. In programming, a parameter is a value that is passed to a subroutine or function for processing.

PDF—Portable **D**ocument **F**ormat (PDF) is a highly compressed multi-platform file format developed by Adobe Systems Incorporated that captures document formatting, text, and images from a variety of applications. This makes it possible for the document to appear the same and print accurately on multiple computers and platforms (unlike many word processors). Viewing a PDF file requires the Adobe Acrobat Reader, a free application distributed by Adobe Systems. There is also a plug-in for viewing PDF files with your web browser. This makes it possible to view PDF files posted on a web site directly instead of having to download them first and then view them with a separate program.

Parse—In linguistics, to parse is to divide language into its grammatical components that can be analyzed. For example, dividing a sentence into verbs, adjectives, nouns, and so on.

In computers, to parse is to divide a computer language statement into parts that can be made useful for the computer. A parser in a compiler is takes each program statement that a developer has written and divides it into parts that can then be used for developing further actions or for creating the instructions that form an executable program.

Alt-N Technologies' MDaemon server and other products often parse email messages to determine their destination or to process them through filters and other tools.

Ping—An acronym for **P**acket **In**ternet **G**roper. It is a basic Internet program used to determine whether a specific IP address is reachable and accepting requests. It does this by sending an Internet Control Message Protocol (ICMP) Echo request and waiting for a response. "Ping" is commonly used as a verb when referring to this process. For example, "I am going to ping that server to see if it is online." "Pinging" an IP address is usually as simple as typing "ping" followed by the IP address or domain at the DOS prompt. For example "Ping 192.0.2.0."

ICMP is addressed in RFC-792 and the Echo protocol is addressed in RFC-862. These can be viewed at:

http://www.rfc-editor.org/rfc/rfc792.txt

http://www.rfc-editor.org/rfc/rfc862.txt

POP—Stands for **P**ost **O**ffice **P**rotocol. POP (also commonly appears as POP3) is the most commonly used email protocol for retrieving email from a mail server. Most email clients use the POP protocol although some also support the newer IMAP protocol as well. POP2 became a standard in the mid 1980s and required SMTP to send messages. It was replaced by the newer version, POP3, which can be used with or without SMTP. POP is sometimes used as a verb when referring to collecting your email from a server. For example, "I'm going to POP my mailbox to get my mail."

POP3 is addressed in RFC-1939, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1939.txt

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Port—In TCP/IP and UDP networks and the Internet, a port is the endpoint of a logical connection and is identified by a number from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged protocols and services. For example, web servers typically are listed on port 80, SMTP servers typically communicate on port 25, and POP servers send and receive mail on 25. Generally, only one program at a time can use, or "bind", to any given port on each machine. When browsing the Internet, oftentimes certain servers will be running on non-default ports, which require you to specify the port in the URL after a colon. For example, "www.example.com:3000."

Port can also be used to refer to the sockets on a computer used for connecting peripheral devices and hardware to it. For example, serial ports, parallel ports, USB ports, and so on.

Finally, port is often used to describe the process of making a program designed for a specific platform or machine function on another platform. For example, "to port a Windows application to UNIX" or "to create a UNIX port for an application."

Post—In Internet messaging, such as email or newsgroups, it is a single message entered into a network communications system for others to see. For example, a message displayed on a newsgroup, mailing list, or discussion board is a post. It can also be used as a verb, as in "post a message to the mailing list or on the newsgroup."

PPP—Stands for "Point to Point Protocol." It is the Internet standard for dial-up connections. PPP is a set of rules that defines how your modem connection exchanges packets of data with other systems on the Internet.

PPP is addressed in RFC-1661, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1661.txt

Protocol—In computing, a protocol is a set of guidelines or standards by which servers and applications communicate. There are many different protocols used for many different purposes, for example, TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP, and so on.

Registry—A database used by Microsoft Windows to store configuration information about software installed on the computer. This includes things like user settings, file extension associations, desktop background, color schemes, and many others. It has the following six parts:

HKEY_User—Stores user information for each user of the system.

HKEY_Current_User—Preferences for the current user.

HKEY_Current_Configuration—Stores settings for the display and printers.

HKEY_Classes_Root—File associations and OLE information.

HKEY_Local_Machine—Hardware, operating system, and installed application settings.

HKEY_Dyn_Data—Performance data.

When programs are installed on your computer the installer usually writes some information to the registry automatically. You can manually edit the registry,

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

however, by using the regedit.exe program that is built in to Windows. But, you should exercise extreme caution when doing this because altering the wrong setting in the registry could cause your computer to function improperly, or not at all.

RFC—Request **F**or **C**omments is the name of the result and the process for creating a standard on the Internet. Each new standard and protocol is proposed and published on the Internet as a "Request For Comments." The Internet Engineering Task Force (IETF) facilitates discussions on the new standard and eventually it is established. In spite of the fact that the standard is established and no further "comments" are "requested," the standard still retains the "Request for Comment" acronym along with its identifying number. For example RFC-822 (now superseded by RFC-2822) is the official standard, or "RFC," for email. However, those protocols that are officially adopted as "standards" do have an official standard number associated with them that is listed in the Internet Official Protocol Standards document (which itself is STD-1 and currently RFC-3700). You can find RFCs on the Internet at many locations but the authoritative source is The RFC Editor, located at http://www.rfc-editor.org/.

The Internet Official Protocol Standards document is located at:

http://www.rfc-editor.org/rfc/std/std1.txt

RTF—Rich **T**ext **F**ormat is a universal file format developed by Microsoft that is supported by nearly all word processors. In contrast to plain text format, RTF enables you to retain formatting, font information, text color, and so on. The file size of RTF files can be very large when compared to other file formats such as Microsoft Word's format (*.doc and *.docx) and Adobe PDF.

Server—A computer, or program, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as an SMTP server, or a machine on which the software is running. A single server *machine* could have many different server *programs* running on it concurrently. For example, your network's server might be running a web server, email server, FTP server, fax server, and others all at once.

SMTP—An acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is the primary protocol used to send email on the Internet from one server to another or from a client to a server. SMTP consists of a set of rules for how a program sending mail and a program receiving mail should interact. Once a server has received email via SMTP it is usually stored there and can then be retrieved by a client via the POP, IMAP, or other protocol.

The SMTP protocol is addressed in RFC-2821, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2821.txt

Spam—Junk mail on the Internet. "Spam" is most commonly used to refer to unsolicited bulk email, although it is often used to refer to any unwanted email in general. A "spammer" will obtain hundreds, thousands, or even millions of email addresses from various sources and then "spam" the list with a message or solicitation. "Spam" can, however, be used to refer to a newsgroup or discussion board posting as well, when the posting is some unwanted or unrelated advertisement for a product or web site.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Spam is quickly becoming a serious problem on the Internet, tying up a great deal of time and server resources. And because spammers oftentimes use various techniques to attempt to mask the origin of the message—such as "spoofing" their addresses to appear to be someone else or attempting to relay the spam covertly through multiple mail servers—preventing it can be a challenge. Alt-N Technologies' MDaemon server is equipped with a number of features designed specifically to aid in fighting spam, such as: DNS Black Lists (DNS-BL), IP Shielding, IP Screening, Relay Control, and others.

The origin of using the term "Spam" to refer to junk email is debated, but it is generally accepted that it comes from a popular Monty Python sketch in which the word "spam" is repeated over and over and periodically accompanied by Vikings singing, "Spam spam spam spam, spam spam spam spam..." However, it may simply be a disparaging comparison to the trademarked Hormel meat product of the same name—everybody gets it at one time or another, but does anyone ever really ask for it?

TCP/IP—Transmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol (TCP/IP) has been described as the foundation of the Internet. It is the basic suite of communication protocols used on the Internet to connect hosts. It is the most commonly used protocol on Local Area Networks as well. It is a two-layer system, the topmost layer being TCP, which manages the disassembling and assembling of files into packets for transmitting over the network. IP, which is the lower layer, handles the addressing of the packets so that they get to the proper destinations. TCP is addressed in the following RFC-793. IP is addressed in RFC-791. These RFCs can be found at:

TCP - http://www.rfc-editor.org/rfc/rfc793.txt

IP - http://www.rfc-editor.org/rfc/rfc791.txt

Telnet—A command and program used to log on to Internet sites that support Telnet access. The Telnet command gets you to the logon prompt of the Telnet server. If you have an account on that server, you can access your permitted resources such as your files, email, and so on. The downside of Telnet is that it is a command line program that uses Unix commands.

The TELNET protocol is addressed in RFCs 854-855, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc854.txt

http://www.rfc-editor.org/rfc/rfc855.txt

Terminal—A device that allows you to send commands to a remote computer. A terminal is a keyboard, display screen, and some simple circuitry. Oftentimes, however, personal computers are used to "emulate" terminals.

Tiff—An acronym for **T**agged **I**mage **F**ile **F**ormat. It is a graphics file format created to be a universal graphics translator across multiple computer platforms. TIFF can handle color depths ranging from 1-bit to 24-bit.

UDP—User **D**atagram **P**rotocol (UDP) is one of the protocols that make up the TCP/IP suite of protocols used for data transfers. UDP is a known as a stateless protocol because it doesn't acknowledge that packets being sent have been received.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

UDP is addressed in RFC-768, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc768.txt

Unix—Unix, or UNIX, is an operating system created by Bell Labs in the 1960s. Designed to be used by many users at the same time, it is the most popular operating system for servers on the Internet. There are now many different operating systems based on UNIX such as Linux, GNU, Ultrix, XENIX, and others.

URL—Every file or server on the Internet has a **U**niform **R**esource **L**ocator (URL). It is the address that you enter into your web browser to get to that server or file. URLs cannot have spaces and always use forward slashes. They have two parts separated by "://". The first part is the protocol being used or resource being addressed (for example, http, telnet, ftp, and so on) and the second part is the Internet address of the file or server (for example, www.altn.com or 127.0.0.1).

Uuencode—A set of algorithms for converting files into a series of 7-bit ASCII characters for transmission over the Internet. Although it stands for Unix-to-Unix encode, it is no longer exclusive to UNIX. It has become a universal protocol used to transfer files between different platforms. It is an encoding method commonly used in email.

WAN—A WAN, or **W**ide **A**rea **N**etwork, is similar to a Local Area Network (LAN) but is usually spread across multiple buildings, or even cities. WANs are sometimes composed of smaller LANs that are interconnected. The Internet could be described as the biggest WAN in the world.

Zip—Refers to a compressed or "zipped" file, usually with the "`.zip`" file extension. "Zipping" is compressing one or more files into a single archive file in order to save space for storage or to facilitate faster transfer to another computer. To use a zip file, however, you'll need to unzip it first with the appropriate program such as PKZIP or WinZip. There are multiple compression/decompression utilities available—both shareware and freeware—from many sites on the Internet. Hopefully you won't have to unzip the utility before you can install it.

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Index

- A -

Access Control List 218, 220, 548
Access Rights 220, 548
Account
  Database Options 628
  Notes 569
  Quotas 638
Account Aliases 613
Account Autoresponders 529
Account Database Options 628, 629
Account Details 521
Account Editor
  Account 529
  Account Details 521
  ActiveSync Client Settings 558
  ActiveSync Clients 562
  ActiveSync Enabling/Disabling 557
  ActiveSync Policy 561
  Administrator Notes 569
  Aliases 546
  Attachments 539
  BlackBerry Enterprise Server 553
  Filters 541
  Folder 524
  Forwarding 533
  Groups 524
  Mail Folder 524
  Mail Services 525
  Mobile Devices 562
  MultiPOP 544
  Notes 569
  Quotas 537
  Restrictions 534
  Settings 573
  Shared Folders 547
  Web Services 526
  White List 571
Account Groups 576, 577
Account Hijack Detection 486
Account Integration 644
Account Manager 518
Account Options
  Passwords 636
Account permissions 526
Account Pruning 537
Account Restrictions 534
Account Signature 568
Accounts 642, 644
  Account-specific BES options 553
  ActiveSync 303
  Autoresponders 617
  BES 328
  BIS 338, 556
  BlackBerry Internet Service 338, 556
  Domain Manager 128
  DomainPOP 90
  Erasing a BlackBerry device 553
  Groups 576, 577
  ODBC Selector Wizard - Account Database 629
  Outlook Connector 627
  Resynchronizing a BlackBerry device 553
  Sending a policy 553
  Slow Sync 328
ACL 220, 548
Activating Outlook Connector 626
Activation 314
Activation options 330
Activation password 553
Active Directory 605, 611
  Authentication 611
  Creating Accounts 605
  Deleting Accounts 605
  Dynamic Authentication 605
  File Security 605
  Monitoring 608
  Persistent Monitoring 605
  Port (Gateway) 170
  Server (Gateway) 170
  Synchronization 608
  Synchronizing with MDaemon 605
  Template 605
  Updating Accounts 605
  Using with Mailing Lists 209
  Verification (Gateway) 170
ActiveSync
  Account Clients 562
  Account Policy 561
  Accounts 303
  Account-specific Client Settings 558
  Account-specific Options 557

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

ActiveSync
Advanced management screens 276
Advanced Options 310, 312
Advanced policy settings 276
Assigned Policy 155
Assigning Policies 292
Auto Discover Service 276
Blacklist 308
Client Settings (Global) 280
Client Settings for Domains 143, 146
Client-level settings 297
Clients 297
Clients (Domain) 156
Client-specific settings 562
Data Wipe 297
Debugging 310
Default Policies 292
Deleting Devices 297
Devices 297
Devices (Domain) 156
Diagnostics 310
Disabling 276
Domain (Clients) 156
Domain Enable/Disable 142
Domain Settings 143, 146
Domains 292
Dumps 310
Enabling 276
Full Wipe 297
Global Settings 280
Logging 312
Managing Clients 280
Policies 284
Policies for Domains 155
Process Dumps 310
Quick access menu items 276
Remotely Wiping a Device 297
Removing Devices 297
Restricting protocols 278
Restrictions 278
Security 308
Soft Wipe 297
Tuning 312
Whitelist 308
Wiping Devices 297
ActiveSync Policy Editor 284
AD 209
AD Authentication 611
adding list members 187
Adding Outlook Connector accounts 627
Address
Blacklist 475
Suppression 475
Address Aliases 546, 613
Address Aliases Settings 615
Address Book Options 105
Address Book Synchronization 224
Address Books 635
Address Verification 640
Address Verification (Gateway) 170
Administrative Roles 570
Template 601
Administrator
Domain 570
Global 570
Notes 569
Administrators 601
Admins/Attachments 375
ADSP 447
Advanced Options
ActiveSync 310, 312
Debugging 310
Diagnostics 310
Dumps 310
Logging ActiveSync 312
Process Dumps 310
Tuning 312
Alias Editor 613
Aliases 546, 613
Aliases Settings 615
ALL_USERS list macro 186
ALL_USERS:<domain> list macro 186
AntiSpam 389
AntiVirus 265, 383, 386, 388, 389
Configuring updater 386, 388
EICAR test message 386, 388
Malware 386, 388
Scheduler 265, 386, 388
Testing 265, 386, 388
Updater 265, 386, 388
Urgent Updates 265, 386, 388
Viewing update report 386, 388
Anti-virus 362
AntiVirus support 362
AntiVirus Updates 265, 267
APOP 53

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Approved List 474
Archival 69
Archiving Logs 115
Archiving mail in a pre 100
ATRN 56, 66, 175
Attachment extension 347
Attachment Linking 262, 539
  BIS 340
  BlackBerry Internet Service 340
Attachment restricting 375
Attachments
  deleting restricted 71
  Template 599
AUTH 66, 442
Authentication 442
Authentication-Results header 447
Authorizing Outlook Connector accounts 627
Auto Discover ActiveSync 276
Auto Response Script Samples 624
Auto Response Scripts 621
Auto-generated a Spam Folder and Filter 428
Automatic
  Gateways 166
  IP Screening 508
  Log Archiving 115
Automatic Learning 409
automatically extracting attachments 262
automatically linking attachments 262
Autoresponder
  Template 590
Autoresponder Exception List 619
Autoresponder Options 620
Autoresponders 529, 617, 621, 624
  Account list 617
  Overview 617
AV
  Alt-N AntiVirus for MDaemon 383
  AntiVirus tab 383
  AntiVirus Updater 386, 388
  SecurityPlus for MDaemon 386, 388
Available Disk Space 349

- B -

Backing up logs 115
Backing up the BES database 329
Backscatter Protection 504
Backscatter Protection - Overview 502
Backup Server 170
Bad Messages 654
Balance 314, 319
Bandwidth 506
Bandwidth Throttling 506, 507
Banners 250
Base Entry DN 209, 611
BATV 502, 504
Bayesian
  Auto-learning 409
  Classification 405
  Learning 409
Bayesian Classification 401
Bayesian Learning 401, 405
BES 314
  Account PIN 328
  Account Status 328
  Accounts 328
  Account-specific options 553
  Activation 314, 328
  Activation options 330
  Activation password 553
  Applying a policy to a domain 326
  Applying a policy to an account 553
  Backup 329
  Calendar options 330
  Database Backup & Retore 329
  Devices 328
  Dialog 314
  Disabling 318
  Domain Policy 326
  Domains 326
  Enabling 318
  Enterprise Activation 314
  Erasing a device 553
  Features 314
  IT Policies 319
  Logging 330
  MDS Connection Service 327
  Options 330
  Overview 314
  Password 553
  PIN 328
  Policies 319
  Policy 553
  Policy Rules 319
  Resending service books 553
  Resetting a device's password 553

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

BES 314
Resetting the calendar 330
Restore 329
Resynchronizing a device 553
Rules 319
Sending a policy 553
Service books 553
Services 318, 330
Setting a Domain's Policy 326
Slow sync 328, 330, 553
SRP 318
Status 318
Stopping when MDaemon stops 330
Synchronization options 330
Verifying SRP 318
Wiping a device 553
Binding 61, 124
BIS 335
Accounts 338, 556
Attachment Linking 340
BlackBerry Internet Service 336
Domains 336
Filtering mail 556
Folders 340
History 336
Inbox 340, 556
Integration 338
Logs 340
Overview 335
Push mail 338, 556
SMTP Server 336
SSL 336
STARTTLS 336
SUBSCRIBE 338
Subscribe URL 336
UNSUBSCRIBE 338
Black List 401, 419
ActiveSync 308
Black Lists 425
BlackBerry Balance 314, 319
BlackBerry Device Activation 314
BlackBerry Enterprise Server 314
Account PIN 328
Account Status 328
Accounts 328
Account-specific options 553
Activation 314, 328
Activation options 330
Activation password 553
Applying a policy to a domain 326
Applying a policy to an account 553
Backup 329
Calendar options 330
Database Backup & Retore 329
Devices 328
Dialog 314
Disabling 318
Domain Policy 326
Domains 326
Enabling 318
Enterprise Activation 314
Erasing a device 553
Features 314
IT Policies 319
Logging 330
MDS Connection Service 327
Options 330
Overview 314
Password 553
PIN 328
Policies 319
Policy 553
Policy Rules 319
Resending service books 553
Resetting a device's password 553
Resetting the calendar 330
Restore 329
Resynchronizing a device 553
Rules 319
Sending a policy 553
Service books 553
Services 318, 330
Setting a Domain's Policy 326
Slow sync 328, 330, 553
SRP 318
Status 318
Stopping when MDaemon stops 330
Synchronization options 330
Verifying SRP 318
Wiping a device 553
BlackBerry Internet Service 335
Accounts 338, 556
Attachment Linking 340
BIS 336
Domains 336
Filtering mail 556

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

BlackBerry Internet Service 335
Folders 340
History 336
Inbox 340, 556
Integration 338
Logs 340
Overview 335
Push mail 338, 556
SMTP Server 336
SSL 336
STARTTLS 336
SUBSCRIBE 338
Subscribe URL 336
UNSUBSCRIBE 338
Blacklist
Address 475
Blacklisted users 475

- C -

Cache 79
Caching IPs 79
CalDAV 243
Calendar 132, 241
Calendar & Scheduling 224
Calendar options
BES 330
BlackBerry Enterprise Server 330
Resetting the BlackBerry calendar 330
Slow Sync 330
Calendar Sync 243
Calendars
CalDAV 243
Canonicalization 453
Catalog control 678
Catalog Editor 650
Certificates 234, 255, 487, 489, 492, 495
SSL 500
Using third-party 500
WorldClient 500
Certification 469, 471
Certification Service Providers 469, 471
Changes in MDaemon 15
Changing WorldClient's Port Setting 228
Choosing your account database 628
Clear message counts at startup 344
Client Settings
ActiveSync 280
ActiveSync Domains 143, 146
Global 280
Clients
ActiveSync (Domain) 156
Domain (ActiveSync) 156
Closing the RAS session 101
Collecting stored SMTP mail 66
ComAgent & IM 130
Composite Log 111
Configuring
DomainPOP Settings 88
IP Cache 79
IP Screen 478
IP Shield 440
MDaemon remotely 251
ODBC Data Source for a List 212
RAS Settings 101
Connection
attempts 101
Profile 103
Connection Window 46
Content Filter 362
Administrators 375, 380
Editor 364
Recipients 380
rules 370
Content Filter & SecurityPlus 362
Content Filter Editor 364
Content-ID header 352
Converting Headers 81
Cookies 229
Copying mail before parsing 100
CRAM-MD5 53
Create Rule Dialog 370
Creating
Auto Response Scripts 621
New Content Filter Rule 366
New ODBC Data Source 631
New System Data Source 214
ODBC data source 631
Site Policy 515
Creating Account Templates 580
Creating and Using SSL Certificates 500
Cryptographic
Signing 446, 450
Verification 446, 447
CSP 469, 471
Customizing DSN messages 661

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Customizing the Queue/Statistic Manager 673
Customizing WorldClient's Banner Images 250

- D -

Daemon 411
Data Source 629, 631
Database Options 628, 629
Date header 352
Debugging
  ActiveSync 310
Deduping Mail 93
Default Domain
  Archival 69
Default headers 93
Defining Content Filter administrators 375
Deleting Account Templates 580
Deleting mail 96
Deleting POP mail after collection 90
Delivery 50
Delivery based on non-address info 99
Delivery Options 50
Delivery Status Notification message 661
Delivery Times 269
Dequeue 66
Dequeue AUTH 66
Dequeuing 175
Dequeuing Gateway Messages 175
Dequeuing Mail 66, 68, 175
Devices
  ActiveSync (Domain) 156
  Domain (ActiveSync) 156
Diagnostics
  ActiveSync 310
Dialup Profile 103
Dialup Settings 101
Digest 199
Disk 349
Disk Space
  Low 349
  Monitoring 349
  Settings 349
disk space limits 177
Display 40
display font 344
DK & DKIM signing 450
DKIM 446, 469, 471
  ADSP 447
  Canonicalization 453
  DNS 450
  including in DMARC reports 468
  Options 453
  Overview 446
  Private Keys 450
  Public Keys 450
  Selectors 450
  Signature tags 453
  Signatures 447
  Signing 450
  tags 453
  Verification 447
DKIM verifying 447
DMARC
  aggregate reports 464
  and Mailing Lists 455
  Creating a DNS record 455
  DNS record 455
  Effect on Mailing Lists 189, 192
  failure reports 464, 468
  filtering messages to Junk E-mail 462
  including DKIM in reports 468
  logging records 468
  Overview 455
  Public suffix file 468
  records 464, 468
  refusing failed messages 462
  Reporting 464, 468
  restrictive policies 462
  tags 464
  Verificaiton 462
DNS
  Black List Exceptions 427
  Black Lists 425
  DMARC Record 455
  Server 58
  Server IP Address 58
DNS Black Lists 426
DNS-BL 425
  Hosts 426
  Options 428
  White List 427
Do Not Disturb 577
Documents Folders
  Allowing or blocking file types 84
  Enabling 84
  Limiting document size 84

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Domain Administrators 570
Domain Gateways 162, 502, 504
Domain Manager 121
  Accounts 128
  ActiveSync 142
  Calendar 132
  Domain Signatures 138
  Host Name & IP 124
  Settings 140
  Signatures 138
  Smart Host 125
  WorldClient Instant Messenger 130
  WorldClient Settings 134
Domain Name Replacement 95
Domain Policy 326
Domain Settings 168
Domain Sharing 75
Domain Signatures 138
DomainKeys Identified Mail 446, 447, 450
DomainPOP 88
  Foreign Mail 98
  Host & Settings 90
  Mail Collection 88
  Name Matching 99
  Parsing 93
  Processing 95
  Routing Rules 96
  Security 100
DomainPOP Mail Collection 88
Domains 513
  Administrators 570
  BES 326
  BIS 336
  BlackBerry Enterprise Server 326
  BlackBerry Internet Service 336
  Creating 121
  Deleting 121
  FQDN 121
  Renaming 121
  Sharing 75
  Trusted 438
Download
  Limits 90, 537
  Size Limits 90, 537
DSN message 661
DSN Settings 661
Duplicate mail 93
Dynamic Authentication 644
Dynamic Screening 482
  WorldClient 237

- E -

Edit Rule 370
Editing
  Gateways 162
  Headers 81
EICAR virus test messages 386, 388
Email Recall 72
Email SSL 487, 489
Enabling
  DomainPOP Mail Collection 90
  Public Folders 87
  WorldClient Server 229
Encryption in WorldClient 224
Enterprise Activation 314
Enterprise Activation password 553
Erasing a BlackBerry device 553
ESMTP 53, 66, 175
ESMTP SIZE command 53
ESMTP VRFY commands 53
ETRN 66, 175
ETRN Dequeue 175
Event Log 114
Event Scheduler 267, 269, 273
Event Tracking Window 40
Exception List
  Autoresponders 619
Excluding addresses from filtering 416
Exclusion List 416
EXPN 53
expressions 370
Extracting Attachments 262, 539

- F -

Faxing 246
File Attachments 539
File Compression 381
Files
  Accessing from a BlackBerry device 327
Filtering mail 556
Filtering Messages 362, 364
Filtering Spam 401, 402, 422
Filters 541

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Fingering an ISP 66
Fixes 351
Flagging Spam 402, 422, 426
Flags 218
fo tag 464
Folder
  Mail 524
Folder access rights 220, 548
Folders 84, 218, 556
Footer 206
Foreign Mail 98
Forwarding 179, 533
  Gateway 165
  Template 594
  to a Domain Gateway 174
Forwarding Mail 96, 533
Free Busy Services 241
Free/Busy Server Options 241

- G -

Gateway 162, 504
  Address Verification 640
  Automatic creation 166
  Domain Settings 168
  Global Gateway Settings 165
  Options 179
  Quotas 177
  Verification 640
Gateway Domain Editor
  Active Directory 170
  Domain Settings 168
  ESMTP ETRN 175
  Forwarding 174
  LDAP 170
  Mail Forwarding 179
  Minger 170
  Quotas 177
  Verification 170
Gateway Manager 162
  Domains 162
  Editor 162
Gateways 502
GatewayUsers.dat file 170
General Email Controls 681
Getting Help 35
Global
  Administrators 570
  Auth 442
  Blacklist 475
Global Gateway Settings 165
Glossary 694
Greylisting 510
Group Manager 576
Group Properties 577
GROUP:<groupname> list macro 186
Groups 524
  Adding an account 576
  Assigning an account template 577
  Creating 576
  Deleting 576
  Do Not Disturb 577
  Instant Messaging 577
  Priority 577
  Removing an account 576
  WorldClient Instant Messenger 577
GUI 40

- H -

Header 206
Header Translation 81
  Exceptions 82
Headers 81, 93, 352
  DMARC and Mailing Lists 192
  List From 192
  List Reply-To 192
  List To 192
  List-Archive 202
  List-Help 202
  List-ID 189, 202
  List-Owner 202
  List-Post 202
  List-Subscribe 202, 354
  List-Unsubscribe 202, 354
  Mailing List 192, 202
Help 35, 40
Help with WorldClient 228
Heuristics 402
Hijack Detection 486
Holding Queue 656
Host Name & IP 124
Host Screening 480
Hosts 426
HTTPS 234, 255, 492, 495

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

- I -

IIS 229, 231
  Running WebAdmin under 258
Images in signatures 83, 138
IMAP 56, 62, 521, 525
  Filters 541
  Folder access rights 220, 548
  Folders 218
  Mail Rules 541
IMAP Folders 556
IMAP message flags 218
IMAP Spam Folder 428
Importing
  Accounts 642, 644
  Accounts From a Text File 642
Inbound Session Threads 64
Instant Messaging 130, 224, 239
Integrated Accounts
  BES 328
  BIS 338
  BlackBerry Enterprise Server 328
  BlackBerry Internet Service 338
  Slow Sync 328
Integration 644
Interface 40
Intranet
  Accessing from a BlackBerry device 327
Introduction 12
IP addresses
  Trusted 439
IP Cache 79
IP Screening 478
  Automatic 508
IP Shield 440
IP Shielding 440
IPv6 61, 124
ISP LAST command 90
ISP Logon Settings 103
ISP POP Accounts 90
IT Policies 319
  Per Domain 326

- L -

LAN Domains 513
LAN IPs 514
Latency 62
LDaemon 105
LDaemon LDAP Server 105
LDAP 105, 106, 209
  Base Entry DN 209, 611
  Gateway verification 165
  Port (Gateway) 170
  Root DN 611
  Root DSE 611
  Root Entry DN 209
  Server (Gateway) 170
  Verification (Gateway) 170
LDAP Database Option 628
LDAP Options 106
LDAP/Address Book Options 105, 106
Learning
  Bayesian 409
Leaving mail at ISP 90
Lightweight Directory Access Protocol 105
Limiting bandwidth 506
Limits 90, 537
Linking Attachments 262, 539
List Moderation 202
List Routing 204
List Security 202
List-Archive header 202
List-Help header 202
List-ID header 202
List-Owner header 202
List-Post header 202
List-Subscribe header 202, 354
List-Unsubscribe header 202, 354
literals 370
Local Queue prepost processing 663
Locking the MDaemon interface 44
Log
  Archiving 115
  Backups 115
  Maintenance 115
Log Mode 109
Log Page 670
Log Settings 116
Logging
  ActiveSync 312
  BES 330
  BIS 340
  BlackBerry Enterprise Server 330

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Logging
BlackBerry Internet Service 340
Composite Log 111
DMARC records 468
Event Log 114
Log Mode 109
Maintenance 115
Reporting 112
Settings 116
Statistics Log 112
Windows Event Log 114
Logging in to WorldClient 228
Logon Name 103
Logon Settings 103
Loop Detection 62
Low Disk Space 349

- M -

Macros
for groups 186
for lists 186
mailing list 186
Message 377
Mail
Custom Queues 658
Filters 541
Forwarding 179, 533
Pruning 537
Queues 84
Rules 541
Mail Folder 524
Mail quotas 638
Mail Release 66, 68
Mail Schedule 273
Mail Sending & Collecting 269
Mail Services 525
Template 585
Mailing List and Catalog Control 678
Mailing Lists
Active Directory 209
adding members 187
ALL_USERS list macro 186
ALL_USERS:<domain> list macro 186
Creating 180
Digest 199
Digest toggle 186
DMARC 189, 455
DMARC and Mailing Lists 192
GROUP:<groupname> list macro 186
Headers 192, 202
List-ID header 189
List-Subscribe header 354
List-Unsubscribe header 354
Members 186
Membership Type 186
Moderating lists 202
Modifying 180
Name 189
Notifications 201
ODBC 211
Post Only toggle 186
Public Folder 208
Read Only toggle 186
Refusing restrictive DMARC messages 189
Routing 204
Security 202
Settings 189
Subscription reminder messages 198
Subscriptions 194
Support Files 206
URLs 202
Using Active Directory with 209
Main Window 40, 344
Maintenance 115
Manager 518
Managing Domains 121
Marking Messages as Spam 426
Max
domains listed 344
messages 177
number of accounts shown 344
number of log lines displayed 344
Maximum Message Hop 62
MDaemon 489
Upgrading 31
MDaemon 15 15
MDaemon and Proxy Servers 692
MDaemon and Text Files 678
MDaemon CA 500
MDaemon Features 12
MDaemon GUI 40
MDaemon Messaging Server 12
MDaemon Technical Support 35
MDaemon's SMTP Work Flow 47
MDS Connection Service 327

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

MDSpamD 411
MDStats Command Line Parameters 674
MDStats.ini File 673
Meetings 241
Members 186
Menu 40
Message Certification 469, 471
Message Filters 541
Message Flags 218
Message Macros 377
Message Recall 72
Message Routing 50
Message size limit 140
Message-ID header 352
metacharacters 370
Migrating Account DBase to ODBC 629
Minger 75, 170, 640
  Gateway verification 165
Mirroring to Windows Address Book 635
Miscellaneous 354
Moderating lists 202
Modify Rule 370
Modifying an Existing Content Filter Rule 370
Monitoring Active Directory 608
Multiple Domains 75
MultiPOP 272, 525, 544

- N -

Name Matching 99
Network Resource Access 356
Network Shares 356
New Accounts template 580
New Features 15
Notepad 678
Notes 569
Notifications 201, 376
  Delivery Status Notification 661
  DSN 661

- O -

ODBC
  Account Database 629
  Data Source 629, 631
  Database Option 628
  Mailing Lists 211
  Selector Wizard - Account Database 629
  System Data Source 212
ODMR 56, 66, 175
Old Mail Pruning 537
On-Demand Mail Relay 66, 175
On-Demand Mail Relay (ODMR) 68
Options
  Autoresponders 620
  Free/Busy Services 241
Order of processing 47
Outbound Session Threads 64
Outbreak Protection 389
Outlook Connector 525
  Accounts 627
  Activating 626
  Adding Users 627
  Authorizing Users 627
  Contact Folders 626
  Generating Shared Folders 626
  Options 626
  Removing Users 627
  Restricting Users 626
Outlook Connector for MDaemon 625
Overview 12

- P -

Parsing
  Deduping Mail 93
  List of parsed headers 93
  Names preceeding email address 99
  parsing 93
  Skipping over 93
Password 103
  Activation 553
  BlackBerry device activation 553
  Enterprise Activation 553
  ISP POP accounts 90
  POP mail account 90
Passwords 636
  Expiration 636
  Strong 636
Performance Enhancements 15
Per-user flags 218
Policies 319, 553
  Account specific 553
  ActiveSync 284, 292
  Assigning to a Domain 155

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Policies 319, 553
Per Domain 326
Sending to a BlackBerry device 553
Policy Rules 319
POP Before SMTP 437
POP DELE command 53
POP mail collection 88
POP Server 90
POP3 525
Ports 56
Post Connection 104
Postmaster
informed when dialup fails 101
receiving summary of non 98
Precedence bulk header 352
Preferences
Disk 349
Fixes 351
Headers 352
Miscellaneous 354
MultiPOP 272
Quotas 638
Servers 53
System 347
UI 344
WAB 635
pre-process list mail 347
Pre-processing 663
Preventing duplicate messages 93
Priority Mail 77
Process 104
Processing 95
Profile 103
Programs 104
Protection
Against backscatter 502, 504
Proxy Servers 692
Pruning 71, 537
Public Catalog 650
Public Folder
Pruning 71
Public Folder Manager 218
Public Folders 84, 87, 547
Mailing Lists 208
Public IMAP Folders 84
Public suffix file 468
Push mail 556

- Q -

QSND 66
Quarantined files
deleting 71
Quarantined messages
deleting 71
Queue and Statistics Manager 664
Queue Page 665
Queue pre-processing 663
Queued Mail 40
Queues 84, 654, 660
Custom 658
Holding 656
Restoring default locations 660
Quotas 177, 537, 638
Template 596

- R -

RAS Dialup 101
Dialup Settings 101
Engine 101
Settings 101
RAS Dialup Settings
ISP Logon Settings 103
Post Connection 104
RAW
Bypassing the Content Filter 682
Message Specification 682
Sample messages 682
Special fields supported by 682
RBL 425
RBL Hosts 426
Real-time Black Lists 425
Recalling a message 72
Received header 93
Recipients 380
Refusing non 98
Regular Expressions 370
Rejecting Spam 402, 422
Relay Control 432
Relay Settings 432
RelayFax
Integration with WorldClient 246
Release Notes 15

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Reminders 241
Mailing List 198
Remote Access and Control 678, 681
Remote Address Verification 640
Remote Administration
Certificates 255, 495
HTTPS 255, 495
SSL 255, 495
Remote Configuration 251, 252
Remote LDAP server 170
Remote Mail Scheduling 269
Remote verification of addresses 170
Renaming Account Templates 580
Report
Quota 638
Report Page 672
Reporting 112, 421
Requirements 12
Resetting the calendar 330
Resources 40
Restore 660
Restoring the BES database from a backup file 329
Restricting ActiveSync Protocols 278
Restricting attachments 375
Restricting IP addresses 61, 124
Restrictions
Account 534
Resynchronizing a device 553
Retrieving stored SMTP mail 66
Retry 654
Retry Queue Settings 654
Return-Receipt-To header 352
Reverse Lookup 434
rf tag 464
ri tag 464
Roles 570
Root DN 209, 611
Root DSE 611
Route Slips 690
Routing 204
Routing mail to various users 96
Routing Rules 96
rua tag 464
ruf tag 464
Rules 96, 541
BES Policy 319
BlackBerry device policy 319
BlackBerry Enterprise Server policy 319
Policy 319
Running WebAdmin under IIS 258
Running WorldClient under IIS6 231

- S -

Saving Mail 100
Scanning for viruses 383
Scheduler 269, 420
AntiVirus updating 265
Custom queue scheduling 269
Event Scheduling 269
Remote Mail Scheduling 269
SecurityPlus updating 265
Spam Filter updates 420
Scheduling AntiVirus Updates 267
Screening 360, 478, 482
WorldClient 237
Screening Hosts 480
Secure Sockets Layer protocol 234, 487, 489, 492, 499, 500
Security 100, 644
Backscatter Protection 504
Backscatter Protection - Overview 502
BATV 502, 504
Dynamic Screening 482
Features 360
Hijack Detection 486
Mailing List 202
Settings 360
SecurityPlus 362
Configuring updater 386, 388
EICAR test message 386, 388
Malware 386, 388
Quarantine 383
Scheduler 265, 386, 388
Testing 265, 386, 388
Updater 265, 386, 388
Urgent Updates 265, 386, 388
Viewing update report 386, 388
virus scanning 383
SecurityPlus for MDaemon 362, 383, 389
Semaphore Files 684
Send & Collect Mail 269
Sender Policy Framework 444
Sender-ID 469, 471
Sending mail to various users 96
Server

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Server
WorldClient 224
Server level administrators 570
Server Settings
Delivery 50
Dequeue 66
DNS 58
Ports 56
Pruning 71
Servers 53
Threads 64
Timers 62
Unknown Mail 73
Servers 53
Service 356
Service books
Resending 553
Services
BES 318, 330
BlackBerry Enterprise Server 318, 330
MDaemon BES 318
Stopping when MDaemon stops 330
Session Threads 64
Session Window 46
Setting a Domain's Policy 326
Setting Download Size Limits 90
Setting IMAP Folder Flags 87
Setting parameters for mail delivery 96
Setting the number if dialup attempts 101
Setting up
Auto Response Scripts 621
DomainPOP Mail Collection 88
Global Blacklist 475
IP Screen 478
IP Shielding 440
RAS 101
Remote configuration 251
Settings
Aliases 615
BES 330
BlackBerry Enterprise Server 330
Domain Manager 140
Template 604
Shared Folders 84, 87, 547
Shared IMAP Folders 87, 218
Shared user folders 220, 548
Sharing Calendars 243
Sharing Domains 75
Sharing mail folders 84
Shortcut Menu 44
Signaling ISP to dequeue mail 66
Signature
Account 568
Signatures
Default 83
Domain 138
HTML 83, 138
Inserting images 83, 138
Plain text 138
Text 83
Signing 450
Signing Messages 446
Simple Message Recall 72
Simple Reporting 421
Site Policy 515
Site Security Policy 515
Size limit
Message 140
Skipping 93
Slow Sync 328
Synchronizing a specific device 553
Smart Host 125
Default 50
SMTP Authentication 50, 442
SMTP call-back 640
SMTP call-forward 640
SMTP Connection Window 46
SMTP RCPT threshold 508
SMTP Work Flow 47
Socket binding 61, 124
Space 349
Spam
Addresses 431
Automatic white listing 413
Bayesian Learning 405
Black List 419, 422
Classification 405
Deleting 402, 422
Directory 405
False negative classification 405
False positive classification 405
Filtering 402, 413, 417, 418, 419, 422
Inserting tag into subject 402
Non-spam directory 405
Rejecting 402, 422
Reporting 421

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Spam
Required score 402
Scoring 402
Simple Reporting 421
Threshold 402
Traps 431
White List 417, 418, 422
Spam Assassin 411
Spam Filter 401, 428
Bayesian Auto-learning 409
Exclusion List 416
MDSpamD 411
Reports 421
Spam Daemon 411
Spam Filtering 422
Updates 420
using and external spam daemon 411
White List 416
Spam Folder 428
Spam Traps 431
SpamD 411
SPF 444, 469, 471
SRP 318
SSL 234, 255, 492, 495
BIS 336
BlackBerry Internet Service 336
MDaemon 489
STARTTLS 499
TLS 499
White List 499
SSL & Certificates 234, 487, 489, 492, 500
SSL Certificates 500
SSL Ports 56
Starting WorldClient 228
STARTTLS 487, 489, 499
BIS 336
BlackBerry Internet Service 336
STARTTLS Required List 500
startup 344
Statistics 40
Statistics Log 112
Status
BlackBerry 318
STLS 487, 489
Stopping a message 72
Subaddressing 541
Subscribe 194, 196
Subscribe header 202, 354
Subscribing To Mailing Lists 196
Subscription reminders 198
Subscriptions 194
Support 35
Support Files 206
Suppressed users 475
Suppression 206
Synchronization 224
Synchronization options
BES 330
BlackBerry Enterprise Server 330
Calendar 330
Slow Sync 330
When activating 330
SyncML 342
Configuring your client 342
System 347
System account email address 347
System Data Source 631
System Requirements 12
System Service 356
system tray 344

- T -

tagged expressions 370
Tags
DKIM 453
DMARC 464
fo 464
fr 464
ri 464
rua 464
ruf 464
Tarpit Settings 508
Tarpit Threshold 508
task bar 344
Task reminders 241
Tasks
CalDAV 243
TCP 56
Technical Support 35
Template Control 582
Template Manager 580
Template Control 582
Template Properties 582
Template Properties 582
Administrative Roles 601

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

Template Properties 582
Attachments 599
Autoresponder 590
Forwarding 594
Mail Services 585
Quotas 596
Settings 604
Web Services 587
White List 602
Templates
Creating 580
Deleting 580
New Accounts 580
Renaming 580
Text Files 678
Third-party Certificates 500
Threading 64
Threads 64
Threshold
Spam rejection 402
Throttling 507
Timeout 62
Timers 62, 269
TLS 487, 489, 499
Toolbar 40
Tray Icon 44
Trusted
Domains 438
Hosts 438
IP addresses 439
Trusted Domains 432
Tuning 312

- U -

UDP 56
UI 344
Undeliverable Mail 654
Unknown Mail 73
Unlocking the MDaemon interface 44
Unsubscribe 194
Unsubscribe header 202, 354
Updates 420
Updating virus definitions 265
Upgrading MDaemon 31
Urgent Updates 265
User Folders 84
User Page 668
Userlist.dat Database Option 628
Using Regular Expressions 370

- V -

VBR 469, 471
Verification
Gateways 170
Remote Address 170
via Active Directory 170
via GatewayUsers.dat file 170
via LDAP 170
via Minger 170
Verifying DKIM 447
Verifying Signatures 446
Verifying SRP Credentials 318
Version 15 15
Virus
Updater 265
Virus:Protection 362
Viruses 389
Vouch-By-Reference 469, 471
VRFY 53, 640

- W -

WAB 635
WCIM 239
Web Access Permissions 526
Web configuration 251
Web Server 229
Web Services
Template 587
WebAdmin 251, 252, 526
Reports 112
Running under IIS 258
WebDAV 243
Welcome File 206
Welcome message subject header 352
What's New? 15
White List 401, 422
ActiveSync 308
Automatic 571
DNS-BL 427
Spam Filter 416
SSL 499
Template 602

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.

White List 401, 422
TLS 499
White List auto 413
White List from 418
White List to 417
Windows Account Integration 644
Windows Address Book 635
Windows Service 356
Wiping a BlackBerry device 553
WorldClient 224, 526
Address Book 247
Branding 250
CalDav 243
Calendar 241
Customizing Banners 250
Date Format 247
Default Language 247
Default Theme 247
Domain Options 239
Domain Settings 247
Dynamic Screening 237
Free/Busy Options 241
Getting Help 228
HTTPS 234, 492
HTTPS Port 234, 492
Instant messaging 239
Logging in 228
Meetings 241
RelayFax integration 246
Reminders 241
Settings 247
Signing in 228
SSL 234, 487, 492
SSL & Certificates 500
Starting WorldClient 228
SyncML 342
Task reminders 241
WCIM 239
Web Server 229
WorldClient SSL 487
WorldClient Documents Folders 84
WorldClient Help 228
WorldClient Instant Messenger 224
WorldClient Settings 134

- X -

X-RBL-Warning headers 352
X-type headers 352

Copyright © 1996-2015. All rights reserved. Alt-N Technologies, Ltd.